

Improved linear programming decoding of LDPC codes and bounds on the minimum and fractional distance

David Burshtein, <i>Senior Member, IEEE</i>	Idan Goldenberg, <i>Student Member, IEEE</i>
School of Electrical Engineering	School of Electrical Engineering
Tel-Aviv University, Tel-Aviv 69978, Israel	Tel-Aviv University, Tel-Aviv 69978, Israel
Email: burstyn@eng.tau.ac.il	Email: idang@eng.tau.ac.il

This research was supported by the Israel Science Foundation, grant no. 772/09.

Improved linear programming decoding of LDPC codes and bounds on the minimum and fractional distance

Abstract—We examine LDPC codes decoded using linear programming (LP). Four contributions to the LP framework are presented. First, a new method of tightening the LP relaxation, and thus improving the LP decoder, is proposed. Second, we present an algorithm which calculates a lower bound on the minimum distance of a specific code. This algorithm exhibits complexity which scales quadratically with the block length. Third, we propose a method to obtain a tight lower bound on the fractional distance, also with quadratic complexity, and thus less than previously-existing methods. Finally, we show how the fundamental LP polytope for generalized LDPC codes and nonbinary LDPC codes can be obtained.

Index Terms—Linear programming decoding, maximum likelihood (ML) decoding, low-density parity-check (LDPC) codes, minimum distance, fractional distance.

I. INTRODUCTION

Within the field of error-correcting codes, the method of linear programming (LP) decoding of linear codes has attracted considerable attention in recent years. Over the past several years, this method has stirred a substantial amount of research. One reason for this is that the LP decoder has the ML certificate property [1], i.e., that if the LP decoder succeeds in producing an integral solution vector, then it produces the ML solution. Another attractive property of the LP decoder is that one may improve the performance in various ways. These include using generic techniques to tighten the LP relaxations [1], using integer programming or mixed integer linear programming [1], [2], adding constraints to the Tanner graph [3] and guessing facets of the polytope [4].

However, LP decoding is disadvantaged as compared to iterative decoding algorithms such as belief propagation or minimum sum decoding because the decoding complexity can be much larger. In general the LP decoder entails a polynomial, non-linear complexity. Several authors have proposed algorithms for low-complexity LP decoding, e.g. [5], [6], [7]. Vontobel and Koetter [5] have proposed an iterative, Gauss-Seidel-type algorithm for approximate LP decoding. In [8] the approach of [5] was studied under a newly-proposed scheduling scheme. This study showed that the performance of the LP decoder can be approached with linear computational complexity. It was also shown that the iterative LP decoder can correct a fixed fraction of errors with linear computational complexity. These results were also extended to generalized LDPC (GLDPC) codes.

In this paper, we present the following main results. First, we show that merging check nodes in the graph can tighten the relaxation and improve the LP decoder. Second, we demonstrate how the linear-complexity LP decoder from [8] can be

used to obtain a lower bound on the minimum distance of a specific code, which is also an upper bound on the fractional distance of the code, with complexity $O(N^2)$, where N is the block length. This lower bound on the minimum distance can be improved by using the check node merging technique. Third, we propose an algorithm which calculates a tight lower bound on the fractional distance with complexity $O(N^2)$. We note that Feldman *et al.* [1] were the first to propose an algorithm which calculates the exact fractional distance; their algorithm entails a complexity which is polynomial but not quadratic in the block length. This is also true for the fractional distance calculation in [7], even though it has reduced complexity as compared to [1]. Our approach has lower complexity as compared to these techniques. Finally, we show how the fundamental polytope of two important classes of codes, namely GLDPC and nonbinary codes, can be obtained. This is accomplished by using the double description method [9], [10]. In addition to these results, we show how the linear-complexity LP decoder can be calculated efficiently for GLDPC codes.

This paper is organized as follows. In section II the linear-complexity LP decoder [8] is reviewed. Section III shows how to perform some computations relating to the linear-complexity LP decoder in an efficient manner. Section IV describes how improved LP decoding can be achieved by merging check nodes. In Section V we propose an algorithm which yields a lower bound on the minimum distance which is also an upper bound on the fractional distance of specific LDPC codes. In Section VI, an algorithm which produces a tight lower bound on the fractional distance is presented. We show how to obtain the fundamental polytope of GLDPC and nonbinary codes in Section VII. Section VIII provides some numerical results, and the paper is concluded in Section IX.

II. APPROXIMATE ITERATIVE LINEAR PROGRAMMING DECODING OF GLDPC CODES

Consider a discrete binary-input memoryless channel (DMC) described by the probability transition function $Q(y|c)$ where c is the transmitted code-bit and y is the channel output. Also consider a GLDPC code \mathcal{C} represented by a Tanner graph with N variable nodes and M linear constraint nodes, where each constraint node represents a small local constituent code, thus generalizing single parity checks (SPCs) in plain LDPC codes. The code \mathcal{C} is used to transmit information over the given DMC. Following the notation in [1], let \mathcal{I} and \mathcal{J} be the sets of variable and constraint nodes, respectively, such that $|\mathcal{I}| = N$ and $|\mathcal{J}| = M$. The variable node $i \in \mathcal{I}$ is connected

to the set \mathcal{N}_i of constraint node neighbors. The constraint node $j \in \mathcal{J}$ is connected to the set \mathcal{N}_j of constraint node neighbors. Further denote by \mathbf{c}_j the vector

$$\mathbf{c}_j \triangleq \{c_i\}_{i \in \mathcal{N}_j}. \quad (1)$$

Given some $j \in \mathcal{J}$, denote by \mathcal{C}_j the constituent binary linear code corresponding to the constraint node $j \in \mathcal{J}$ (thus for plain LDPC codes, \mathcal{C}_j is a simple parity-check code). Let $\mathbf{0}_j$ denote the all-zero local codeword on constraint node j , and let $\mathbf{0}$ denote the all-zero codeword in \mathcal{C} . A valid codeword $\mathbf{c} \in \mathcal{C}$ satisfies $\mathbf{c}_j \in \mathcal{C}_j, \forall j \in \mathcal{J}$.

We assume, without loss of generality, that there are no parallel edges in the Tanner graph, since otherwise we can modify the structure of the code to satisfy this constraint.

The LP decoder is given by [1],

$$\hat{\mathbf{c}} \triangleq \underset{\mathbf{c}, \boldsymbol{\omega}}{\operatorname{argmin}} P(\mathbf{c}) \quad (2)$$

where the vector $\boldsymbol{\omega}$ is defined by

$$\boldsymbol{\omega} \triangleq \{w_{j,\mathbf{g}}\}_{j \in \mathcal{J}, \mathbf{g} \in \mathcal{C}_j}$$

and where

$$P(\mathbf{c}) \triangleq \sum_{i \in \mathcal{I}} c_i \gamma_i \quad (3)$$

subject to

$$w_{j,\mathbf{g}} \geq 0 \quad \forall j \in \mathcal{J}, \mathbf{g} \in \mathcal{C}_j \quad (4)$$

$$\sum_{\mathbf{g} \in \mathcal{C}_j} w_{j,\mathbf{g}} = 1 \quad \forall j \in \mathcal{J} \quad (5)$$

$$c_i = \sum_{\mathbf{g} \in \mathcal{C}_j, g_i=1} w_{j,\mathbf{g}} \quad \forall j \in \mathcal{J}, i \in \mathcal{N}_j \quad (6)$$

and where

$$\gamma_i \triangleq \log \frac{Q(y_i | 0)}{Q(y_i | 1)}$$

where all logarithms henceforth are to the base e . We assume that there are no perfect measurements from the channel, i.e.

$$-\infty < \gamma_i < \infty \quad \forall i \in \mathcal{I}. \quad (7)$$

Note that if we transmit over the binary erasure channel (BEC) then this assumption does not hold. However, we can re-normalize the γ_i 's by replacing $\gamma_i = \infty$ with $\gamma_i = 1$ and $\gamma_i = -\infty$ with $\gamma_i = -1$. After this re-normalization the assumption (7) holds, and we can then apply the decoding algorithm.

We term the minimization problem (2)-(6), *Problem-P*. We also define

$$\boldsymbol{\omega}_j \triangleq \{w_{j,\mathbf{g}}\}_{\mathbf{g} \in \mathcal{C}_j}$$

The polytope $\mathcal{Q}_j(\mathcal{C})$ is defined as follows [1]: $\mathbf{c} \in \mathcal{Q}_j(\mathcal{C})$ (sometimes we will use the notation $\mathbf{c}_j \in \mathcal{Q}_j(\mathcal{C})$, the meaning will be clear from the context) if and only if there exists a vector $\boldsymbol{\omega}_j$ such that (4)-(6) hold for this value of j . For plain LDPC codes it was shown that $\mathbf{c} \in \mathcal{Q}_j(\mathcal{C})$ if and only if

$$\begin{aligned} 0 \leq c_i \leq 1 & \quad \forall i \in \mathcal{N}_j \\ \sum_{i \in \mathcal{N}_j \setminus S} c_i + \sum_{i \in S} (1 - c_i) \geq 1 & \quad \forall S \subseteq \mathcal{N}_j, |S| \text{ odd} \end{aligned} \quad (8)$$

We further denote by $\mathcal{Q}(\mathcal{C}) \triangleq \bigcap_{j \in \mathcal{J}} \mathcal{Q}_j(\mathcal{C})$ the relaxed [1] or fundamental polytope. Thus \mathbf{c} is feasible in (4)-(6) if and only if $\mathbf{c} \in \mathcal{Q}(\mathcal{C})$. We thus have, in addition to (2), the relation

$$\hat{\mathbf{c}} = \underset{\mathbf{c} \in \mathcal{Q}(\mathcal{C})}{\operatorname{argmin}} P(\mathbf{c}) \quad (9)$$

An important observation is that the LP decoder has the ML certificate [1] in the sense that if the solution of Problem-P is integer (in fact an integer $\boldsymbol{\omega}$ implies that \mathbf{c} is also integer by (6)) then it is the ML decision.

Now consider the following problem, which we term *Problem-D*. The variables in this problem are

$$\mathbf{u} = \{u_{i,j}\}_{i \in \mathcal{I}, j \in \mathcal{N}_i}$$

and the problem is defined by

$$\max_{\mathbf{u}} D(\mathbf{u}) \quad \text{where} \quad D(\mathbf{u}) \triangleq \sum_{j \in \mathcal{J}} \min_{\mathbf{g} \in \mathcal{C}_j} \left\{ \sum_{i \in \mathcal{N}_j} u_{i,j} g_i \right\} \quad (10)$$

subject to

$$\sum_{j \in \mathcal{N}_i} u_{i,j} = \gamma_i \quad \forall i \in \mathcal{I}. \quad (11)$$

Lemma 1: Problem-P and Problem-D are Lagrange dual problems. The minimum of Problem-P is equal to the maximum of Problem-D.

The lemma is proven in [8].

Vontobel and Koetter [5] have proposed an algorithm which yields an approximated solution to Problem-D. They suggested to consider the following “soft” version of Problem-D, termed *Problem-DS*:

$$\max_{\mathbf{u}} DS(\mathbf{u})$$

where

$$DS(\mathbf{u}) \triangleq -\frac{1}{K} \sum_{j \in \mathcal{J}} \log \sum_{\mathbf{g} \in \mathcal{C}_j} e^{-K \sum_{i \in \mathcal{N}_j} u_{i,j} g_i} \quad (12)$$

subject to (11). Note that the objective function in (12) is obtained from (10) by approximating the $\min()$ function using a log-sum-exp function with a parameter $K > 0$. This approximation can become arbitrarily accurate by increasing K . Also note that $DS(\mathbf{u})$ is concave since the log-sum-exp function is convex. In what follows, we give a brief overview of the linear-complexity iterative LP decoder. The reader is referred to [8] for additional details.

Let $\tilde{\Psi}^j$ denote the $(|\mathcal{N}_j| + 1) \times |\mathcal{C}_j|$ matrix

$$\tilde{\Psi}^j \triangleq \begin{pmatrix} \mathbf{1}_{|\mathcal{C}_j|} \\ \Psi^j \end{pmatrix} \quad (13)$$

where $\mathbf{1}_{|\mathcal{C}_j|}$ is a row vector of $|\mathcal{C}_j|$ ones and the columns of Ψ^j are all the codewords of \mathcal{C}_j .

Note that the equation set

$$\begin{pmatrix} 1 \\ \mathbf{c}_j \end{pmatrix} = \tilde{\Psi}^j \boldsymbol{\omega}_j$$

expresses the constraints (5)-(6). We define

$$\Xi^j \triangleq \left(\tilde{\Psi}^j \right)^T \left(\tilde{\Psi}^j \left(\tilde{\Psi}^j \right)^T \right)^{-1}$$

where A^T is the transpose of matrix A , and

$$\eta \triangleq \max_j \left\{ |\mathcal{C}_j| |\mathcal{N}_j| \max_{l,i} |\Xi_{l,i}^j| \right\}$$

where $\Xi_{l,i}^j$ is the (l,i) element of Ξ^j .

Now let $\epsilon > 0$ be a constant such that $\epsilon \leq 1/\eta$. We define

$$\tilde{\lambda}_i \triangleq \lambda_i(1 - \eta\epsilon) + \frac{\eta}{2}\epsilon \quad \forall i \in \mathcal{I} \quad (14)$$

and

$$\tilde{\lambda} \triangleq \{\tilde{\lambda}_i\}_{i \in \mathcal{I}}.$$

We will also define the quantities

$$\begin{aligned} A_{k,j} &\triangleq \sum_{\mathbf{g} \in \mathcal{C}_j, g_k=1} e^{-K \sum_{i \in \mathcal{N}_j \setminus k} u_{i,j} g_i} \\ B_{k,j} &\triangleq \sum_{\mathbf{g} \in \mathcal{C}_j, g_k=0} e^{-K \sum_{i \in \mathcal{N}_j \setminus k} u_{i,j} g_i} \end{aligned} \quad (15)$$

The following iterative algorithm was proposed in [8] to find an approximate solution to Problem-P in linear time complexity.

Algorithm 1: Given a GLDPC code, channel observations and some fixed parameters $\epsilon_0 \in (0, 1/\eta)$ and $K > 0$ do:

1) **Initialization:**

$$\begin{aligned} \forall i \in \mathcal{I}, j \in \mathcal{N}_i : u_{i,j} &= \gamma_i / |\mathcal{N}_i| \\ \forall i \in \mathcal{I}, j \in \mathcal{N}_i : v_{i,j} &= -\frac{1}{K} \log \frac{B_{i,j}}{A_{i,j}} \\ \forall i \in \mathcal{I}, j \in \mathcal{N}_i : \lambda_{i,j} &= \frac{1}{1 + e^{K(u_{i,j} - v_{i,j})}} \\ \forall i \in \mathcal{I} : \lambda_i &= \frac{1}{|\mathcal{N}_i|} \sum_{j \in \mathcal{N}_i} \lambda_{i,j} \\ \forall i \in \mathcal{I} : \epsilon_i &= \max_{j \in \mathcal{N}_i} |\lambda_{i,j} - \lambda_i| \\ \mathcal{A} &= \{i \in \mathcal{I} : \epsilon_i \geq \epsilon_0\} \end{aligned}$$

2) **Iteration:** Pick an arbitrary element $k \in \mathcal{A}$ and make the following updates:

$$\begin{aligned} \forall j \in \mathcal{N}_k : u_{k,j} &= v_{k,j} + \frac{\gamma_k}{|\mathcal{N}_k|} - \frac{1}{|\mathcal{N}_k|} \sum_{l \in \mathcal{N}_k} v_{k,l} \\ \forall i \in \mathcal{N}_j \setminus k, j \in \mathcal{N}_k : v_{i,j} &= -\frac{1}{K} \log \frac{B_{i,j}}{A_{i,j}} \\ \forall i \in \mathcal{N}_j, j \in \mathcal{N}_k : \lambda_{i,j} &= \frac{1}{1 + e^{K(u_{i,j} - v_{i,j})}} \\ \forall i \in \mathcal{N}_j, j \in \mathcal{N}_k : \lambda_i &= \frac{1}{|\mathcal{N}_i|} \sum_{j' \in \mathcal{N}_i} \lambda_{i,j'} \\ \forall i \in \mathcal{N}_j, j \in \mathcal{N}_k : \epsilon_i &= \max_{j' \in \mathcal{N}_i} |\lambda_{i,j'} - \lambda_i| \\ \forall i \in \mathcal{N}_j, j \in \mathcal{N}_k : \text{If } i \in \mathcal{A} \text{ and } \epsilon_i < \epsilon_0 &\text{ then } \mathcal{A} = \mathcal{A} \setminus i \\ \forall i \in \mathcal{N}_j, j \in \mathcal{N}_k : \text{If } i \notin \mathcal{A} \text{ and } \epsilon_i \geq \epsilon_0 &\text{ then } \mathcal{A} = \mathcal{A} \cup i \end{aligned}$$

3) **Loop Control:** If $\mathcal{A} \neq \emptyset$ then repeat step 2. Otherwise proceed to step 4.

4) **Produce the final solution and Exit:** $\forall i \in \mathcal{I}$: Compute $\tilde{\lambda}_i$ using (14), and \hat{c}_i using

$$\hat{c}_i = \begin{cases} 1 & \text{if } \tilde{\lambda}_i > 0.5 \\ 0 & \text{if } \tilde{\lambda}_i < 0.5 \end{cases}$$

Output the primal vector $\tilde{\lambda}$, the dual vector \mathbf{u} and the bitwise-estimated integral vector $\{\hat{c}_i\}_{i \in \mathcal{I}}$

Note that each edge in the graph connecting the variable node i and the constraint node j is associated with the variables $u_{i,j}$, $v_{i,j}$ and $\lambda_{i,j}$. Each variable node $i \in \mathcal{I}$ is associated with the variables λ_i , $\tilde{\lambda}_i$, \hat{c}_i and ϵ_i . In [8] the following assumptions were made.

1)

$$|\gamma_i| \leq \gamma_{\max} \quad \forall i \in \mathcal{I} \quad (16)$$

for some positive constant γ_{\max} . Note that practical channels with non-perfect measurements, that satisfy (7), also satisfy (16), since their output is quantized to some finite set.

2) As was indicated earlier, we can assume without loss of generality that there are no parallel edges in the Tanner graph.

3) We assume that $d'_j \geq 3 \forall j \in \mathcal{J}$. where d'_j is the dual distance of the constituent code corresponding to the constraint node j . For plain LDPC codes this assumption degenerates to $|\mathcal{N}_j| \geq 3 \forall j \in \mathcal{J}$ (this simpler version appears also in [5]).

4) We assume that all node degrees are bounded by some constant (independent of N).

Under these assumptions it was shown in [8], for any fixed $\epsilon_0 \in (0, 1/\eta)$ and $K > 0$, that Algorithm 1 exits after $O(N)$ iterations, and that the vector $\tilde{\lambda}$ is feasible in Problem-P. Furthermore, by setting K sufficiently large and ϵ_0 sufficiently small, we can make $(P(\tilde{\lambda}) - P^*)/N$, where P^* is the minimum value of Problem-P, arbitrarily small. More precisely,

[8, Theorem 1]: Consider Algorithm 1 under the four assumptions above. For any given δ , after $O(N)$ iterations, each with a constant number of operations, the algorithm yields a vector, $\tilde{\lambda}$, which is feasible in Problem-P and satisfies

$$0 \leq P(\tilde{\lambda}) - P^* \leq \delta N \quad (17)$$

By weak duality and by the primal feasibility of $\tilde{\lambda}$, we have

$$D(\mathbf{u}) \leq P^* \leq P(\tilde{\lambda}) \quad (18)$$

We will make use of the fact that P^* is sandwiched between the lower bound $D(\mathbf{u})$ and the upper bound $P(\tilde{\lambda})$. In fact, in the proof of [8, Theorem 1], it was shown that

$$P(\tilde{\lambda}) - D(\mathbf{u}) \leq \delta N \quad (19)$$

and thus follows the result of the theorem.

III. EFFICIENT COMPUTATIONS RELATED TO THE ITERATIVE APPROXIMATE LP DECODER

In this section, we demonstrate how the computation of $A_{k,j}$ and $B_{k,j}$, defined in (15) can be efficiently implemented for GLDPC codes. For LDPC codes an efficient computation scheme was presented in [8]. We also show how to efficiently implement the calculation of $D(\mathbf{u})$.

We follow the approach proposed in [11] that uses a trellis representation of the code. To simplify the notation we assume that $\mathcal{N}_j = \{0, 1, \dots, n-1\}$, and we fix j and omit it from

$A_{k,j}$, $B_{k,j}$, C_j and $u_{i,j}$. In addition we assume that the code C_j is represented by the parity check matrix

$$H = [\mathbf{h}_0 \mathbf{h}_1 \dots \mathbf{h}_{n-1}]$$

with columns $\mathbf{h}_0, \mathbf{h}_1, \dots, \mathbf{h}_{n-1}$, such that the vectors \mathbf{h}_i are m -dimensional binary vectors representing elements of the field $\text{GF}(2^m)$.

A. Efficient Computation of $A_{k,j}$ and $B_{k,j}$

We need to compute A_k and B_k , $k = 0, 1, \dots, n-1$, defined by

$$\begin{aligned} A_k &\triangleq \sum_{\mathbf{g}: H\mathbf{g}=0, g_k=1} e^{-K(\sum_{i=0}^{n-1} u_i g_i - u_k)} \\ B_k &\triangleq \sum_{\mathbf{g}: H\mathbf{g}=0, g_k=0} e^{-K \sum_{i=0}^{n-1} u_i g_i} \end{aligned} \quad (20)$$

where $\mathbf{g} \triangleq [g_0, g_1, \dots, g_{n-1}]^T$

Let H_k , \mathbf{g}_k , $E(k, \mathbf{s})$ and $E(k, \mathbf{s}, b)$ be defined by

$$\begin{aligned} H_k &\triangleq [\mathbf{h}_0 \mathbf{h}_1 \dots \mathbf{h}_k] \quad , \quad \mathbf{g}_k \triangleq [g_0, g_1, \dots, g_k]^T \\ E(k, \mathbf{s}) &= \sum_{\mathbf{g}_k: H_k \mathbf{g}_k = \mathbf{s}} e^{-K \sum_{i=0}^k u_i g_i} \end{aligned} \quad (21)$$

and

$$\begin{aligned} E(k, \mathbf{s}, b) &= \sum_{\mathbf{g}_k: H_k \mathbf{g}_k = \mathbf{s}, g_k=b} e^{-K \sum_{i=0}^k u_i g_i} \\ &= E(k-1, \mathbf{s} \oplus b \cdot \mathbf{h}_k) e^{-K u_k \cdot b} \end{aligned} \quad (22)$$

In these definitions \mathbf{s} is an m dimensional binary vector, representing an element in $\text{GF}(2^m)$, $b \in \{0, 1\}$, $g_i \in \{0, 1\}$, and \oplus is the bitwise exclusive or operator (addition in $\text{GF}(2^m)$).

Similarly we define

$$\begin{aligned} \tilde{H}_k &\triangleq [\mathbf{h}_{k+1} \mathbf{h}_{k+2} \dots \mathbf{h}_{n-1}] \\ \tilde{\mathbf{g}}_k &\triangleq [g_{k+1}, g_{k+2}, \dots, g_{n-1}]^T \\ \tilde{E}(k, \mathbf{s}) &= \sum_{\tilde{\mathbf{g}}_k: \tilde{H}_k \tilde{\mathbf{g}}_k = \mathbf{s}} e^{-K \sum_{i=k+1}^{n-1} u_i g_i} \end{aligned} \quad (23)$$

$E(k, \mathbf{s})$ and $\tilde{E}(k, \mathbf{s})$ can be computed recursively using the forward recursion for $k = 0, 1, \dots, n-1$

$$E(k, \mathbf{s}) = E(k-1, \mathbf{s}) + E(k-1, \mathbf{s} \oplus \mathbf{h}_k) \cdot e^{-K u_k} \quad (24)$$

(for a given value of k we use this recursion to compute $E(k, \mathbf{s})$ for all possible states \mathbf{s}) and the backward recursion for $k = n-2, \dots, 1, 0$

$$\tilde{E}(k, \mathbf{s}) = \tilde{E}(k+1, \mathbf{s}) + \tilde{E}(k+1, \mathbf{s} \oplus \mathbf{h}_{k+1}) \cdot e^{-K u_{k+1}} \quad (25)$$

and the initial conditions

$$E(-1, \mathbf{s}) = \begin{cases} 1, & \mathbf{s}=0 \\ 0, & \text{otherwise} \end{cases} \quad (26)$$

and

$$\tilde{E}(n-1, \mathbf{s}) = \begin{cases} 1, & \mathbf{s}=0 \\ 0, & \text{otherwise} \end{cases} \quad (27)$$

Finally, A_k and B_k are computed using

$$A_k = e^{K u_k} \sum_{\mathbf{s}} E(k, \mathbf{s}, 1) \tilde{E}(k, \mathbf{s}) \quad (28)$$

and

$$B_k = \sum_{\mathbf{s}} E(k, \mathbf{s}, 0) \tilde{E}(k, \mathbf{s}) \quad (29)$$

for $k = 0, \dots, n-1$.

In practice, in order to avoid numerical problems, the forward recursion (24) and the backward recursion (25) are computed using logarithmic computation.

Another possibility is to use the method proposed by Hartmann and Rudolph [12]. However, in this case one faces a numerical problem since the method involves subtractions, and not only summations.

B. Efficient calculation of $D(\mathbf{u})$

To calculate $D(\mathbf{u})$ for GLDPC codes, we use the same methodology as in the calculation of $A_{k,j}$ and $B_{k,j}$, and we use the definitions of H_k and \mathbf{g}_k in (21). The difference is that here we only need a forward recursion for the calculation.

By defining

$$A(k, \mathbf{s}) \triangleq \min_{\mathbf{g}_k: H_k \mathbf{g}_k = \mathbf{s}} \sum_{i=0}^{n-1} u_i g_i$$

it is easily seen that our objective (the minimization in (10)) is equal to

$$A(n-1, 0) \quad (30)$$

Now, $A(k, \mathbf{s})$ can be calculated recursively for $k = 0, 1, \dots, n-1$ as

$$A(k, \mathbf{s}) = \min(A(k-1, \mathbf{s}), A(k-1, \mathbf{s} \oplus \mathbf{h}_k) + u_k)$$

with the initial conditions

$$A(-1, \mathbf{s}) = \begin{cases} 0, & \mathbf{s}=0 \\ \infty, & \text{otherwise} \end{cases} \quad (31)$$

IV. A NEW METHOD FOR IMPROVED LP DECODING

Consider some GLDPC code \mathcal{C} with an underlying Tanner graph \mathcal{G} . Let $\hat{\mathbf{c}}$ be the LP decoded word considered in Section II, i.e.

$$\hat{\mathbf{c}} = \underset{\mathbf{c} \in \mathcal{Q}(\mathcal{C})}{\text{argmin}} P(\mathbf{c})$$

where

$$\mathcal{Q}(\mathcal{C}) = \left\{ \mathbf{c} : \exists \boldsymbol{\omega} = \{w_{j,S}\}_{j \in \mathcal{J}, S \in \mathcal{E}_j} \text{ s.t. (4), (5) and (6) hold} \right\}$$

Now suppose that we merge some of the constraint nodes together to form an alternative representation of the given code, with underlying graph \mathcal{G}' . This is illustrated in Figure 1, where we merge the constraint nodes j_1 and j_2 into j'_1 (i.e. the constituent code associated with j'_1 satisfies both the constraints implied by j_1 and those implied by j_2), and the constraint nodes j_3 and j_4 into j'_2 . In this example the constraint node j_5 is left unchanged (j'_3 in \mathcal{G}').

Denote by \mathcal{J}' the new set of constraint nodes corresponding to \mathcal{G}' . Now, we can apply the LP relaxation to the new representation and calculate $\hat{\mathbf{c}}'$ defined by,

$$\hat{\mathbf{c}}' = \underset{\mathbf{c} \in \mathcal{Q}'(\mathcal{C})}{\text{argmin}} P(\mathbf{c})$$

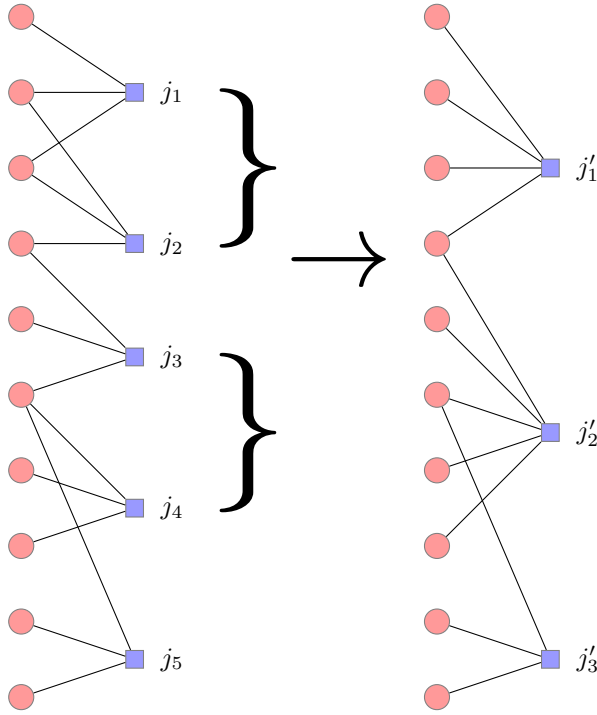


Fig. 1. Starting from the graph \mathcal{G} on the left part of the figure that represents the code \mathcal{C} , we merge constraint nodes, thus creating a new representation of \mathcal{C} with an underlying graph \mathcal{G}' shown on the right.

where

$$\mathcal{Q}'(\mathcal{C}) = \left\{ \mathbf{c} : \exists \boldsymbol{\omega} = \{w'_{j,\mathbf{g}}\}_{j \in \mathcal{J}', \mathbf{g} \in \mathcal{C}'_j} \text{ s.t. (4), (5)} \right. \\ \left. \text{and (6) (with } \mathcal{J}', \mathcal{C}'_j \text{ instead of } \mathcal{J}, \mathcal{C}_j) \text{ hold} \right\}$$

Proposition 1: $\mathcal{Q}'(\mathcal{C}) \subseteq \mathcal{Q}(\mathcal{C})$.

Proof: Suppose that $\mathbf{c} \in \mathcal{Q}'(\mathcal{C})$. We need to show that $\mathbf{c} \in \mathcal{Q}(\mathcal{C})$. First suppose that the only difference between \mathcal{G} and \mathcal{G}' is that the constraint nodes $j_1, j_2, \dots, j_r \in \mathcal{J}$ in \mathcal{G} are merged to form the constraint node $j' \in \mathcal{J}'$ in \mathcal{G}' . All the other constraint nodes in \mathcal{G} and \mathcal{G}' are identical (i.e. they are associated with the same constituent codes and are connected to the same variable nodes). Now, there exists $\{w'_{j,\mathbf{g}}\}_{j \in \mathcal{J}', \mathbf{g} \in \mathcal{C}'_j}$ such that (4), (5) and (6) (with $\mathcal{J}', \mathcal{C}'_j$ instead of $\mathcal{J}, \mathcal{C}_j$) hold. For $j = j_1, j_2, \dots, j_r$, define $w_{j,\mathbf{g}}$ by,

$$w_{j,\mathbf{g}} \triangleq \sum_{\mathbf{g}' \in \mathcal{C}'_j, \mathbf{g}_{\mathcal{N}_j} = \mathbf{g}} w'_{j',\mathbf{g}'}$$

where $\mathbf{g}_{\mathcal{N}_j}$ is the sub-codeword \mathbf{g}' restricted to indices $i \in \mathcal{N}_j$. For all other values of $j \in \mathcal{J}$ we define $w_{j,\mathbf{g}} = w'_{j'(j),\mathbf{g}}$ where $j'(j) \in \mathcal{J}'$ is the constraint node in \mathcal{G}' that corresponds to the constraint node $j \in \mathcal{J}$ in \mathcal{G} .

Note that $\mathbf{g}' \in \mathcal{C}'_j$ only if $\mathbf{g}_{\mathcal{N}_j} \in \mathcal{C}_j$ (since any codeword associated with the merged node j' is a codeword of \mathcal{C}_j for all $j = j_1, \dots, j_r$). It follows that for all $j = j_1, \dots, j_r$,

$$w_{j,\mathbf{g}} \geq 0 \\ \sum_{\mathbf{g} \in \mathcal{C}_j} w_{j,\mathbf{g}} = \sum_{\mathbf{g}' \in \mathcal{C}'_j} w'_{j',\mathbf{g}'} = 1$$

$$\sum_{\mathbf{g} \in \mathcal{C}_j, g_i=1} w_{j,\mathbf{g}} = \sum_{\mathbf{g}' \in \mathcal{C}'_j, g'_i=1} w'_{j',\mathbf{g}'} = c_i \quad \forall i \in \mathcal{N}_j$$

Hence we conclude that $\mathbf{c} \in \mathcal{Q}(\mathcal{C})$. We have therefore shown that in this case $\mathcal{Q}'(\mathcal{C}) \subseteq \mathcal{Q}(\mathcal{C})$.

Now suppose that \mathcal{G}' is formed by a general merge up of constraint nodes in \mathcal{G} . In this case the process of constructing \mathcal{G}' from \mathcal{G} can be separated to a series of merge up steps of constraint nodes, such that at each step we merge a single set of parity check nodes from the graph constructed so far in order to form a new graph. That is, starting from $\mathcal{G} = \tilde{\mathcal{G}}_1$, we first construct $\tilde{\mathcal{G}}_2$ with the polytope $\tilde{\mathcal{Q}}_2$. Then we construct $\tilde{\mathcal{G}}_3$ with the polytope $\tilde{\mathcal{Q}}_3$ and so forth, until we obtain $\tilde{\mathcal{G}}_s = \mathcal{G}'$ with the polytope $\tilde{\mathcal{Q}}_s = \mathcal{Q}'(\mathcal{C})$. For $i = 1, 2, \dots, s-1$, the graph $\tilde{\mathcal{G}}_{i+1}$ is obtained from $\tilde{\mathcal{G}}_i$ by merging a single set of constraint nodes into one constraint node and leaving all the other constraint nodes intact (e.g., in the example shown in Figure 1, $\tilde{\mathcal{G}}_1 = \mathcal{G}$ is the graph shown on the left. We first merge j_1 and j_2 into j'_1 , thus forming $\tilde{\mathcal{G}}_2$. Then we merge j_3 and j_4 into j'_2 thus forming $\tilde{\mathcal{G}}_3 = \mathcal{G}'$, which is the graph shown on the right). By what we have shown so far we know that,

$$\mathcal{Q}'(\mathcal{C}) = \tilde{\mathcal{Q}}_s \subseteq \tilde{\mathcal{Q}}_{s-1} \subseteq \dots \subseteq \tilde{\mathcal{Q}}_1 = \mathcal{Q}(\mathcal{C})$$

□

Note that when we merge all the constraint nodes into one constraint node, the resulting polytope, $\mathcal{Q}^{\text{ML}}(\mathcal{C})$, is the convex combination of all possible codewords. That is, the set of vertices of this polytope is the set of codewords of \mathcal{C} , and the minimization of $P(\mathbf{c})$ over $\mathbf{c} \in \mathcal{Q}^{\text{ML}}(\mathcal{C})$ yields the ML decoded codeword. Thus we have $\mathcal{Q}^{\text{ML}}(\mathcal{C}) \subseteq \mathcal{Q}'(\mathcal{C}) \subseteq \mathcal{Q}(\mathcal{C})$. Note also that for any codeword \mathbf{c} we have $\mathbf{c} \in \mathcal{Q}(\mathcal{C})$, $\mathbf{c} \in \mathcal{Q}'(\mathcal{C})$ and $\mathbf{c} \in \mathcal{Q}^{\text{ML}}(\mathcal{C})$. That is, $\mathcal{Q}'(\mathcal{C})$ is a finer relaxation of $\mathcal{Q}^{\text{ML}}(\mathcal{C})$ than $\mathcal{Q}(\mathcal{C})$.

Let the error probability $P_e(\mathbf{c})$ of the decoder that uses the initial graph \mathcal{G} , given that the transmitted codeword is \mathbf{c} , be defined by,

$$P_e(\mathbf{c}) = \Pr(\exists \tilde{\mathbf{c}} \in \mathcal{Q}(\mathcal{C}) : \tilde{\mathbf{c}} \neq \mathbf{c}, P(\tilde{\mathbf{c}}) \leq P(\mathbf{c}))$$

Similarly, the error probability $P_e(\mathbf{c})$ of the decoder that uses the graph \mathcal{G}' , given that the transmitted codeword is \mathbf{c} , is defined by,

$$P'_e(\mathbf{c}) = \Pr(\exists \tilde{\mathbf{c}} \in \mathcal{Q}'(\mathcal{C}) : \tilde{\mathbf{c}} \neq \mathbf{c}, P(\tilde{\mathbf{c}}) \leq P(\mathbf{c}))$$

By proposition 1 we immediately obtain the following,

Proposition 2: $P'_e(\mathbf{c}) \leq P_e(\mathbf{c})$.

This proposition holds trivially due to the fact that the second LP decoder uses a tighter relaxation of $\mathcal{Q}^{\text{ML}}(\mathcal{C})$.

Proposition 3: Suppose that in the merging process of constraint nodes we only merge constraint nodes j_1, \dots, j_r such that the subgraph of \mathcal{G} induced by j_1, \dots, j_r and their direct neighbors is cycle free. Then $\mathcal{Q}(\mathcal{C}) = \mathcal{Q}'(\mathcal{C})$ and $P_e(\mathbf{c}) = P'_e(\mathbf{c})$.

Proof: We already know from Proposition 1 that $\mathcal{Q}'(\mathcal{C}) \subseteq \mathcal{Q}(\mathcal{C})$. Thus we only need to show that $\mathcal{Q}(\mathcal{C}) \subseteq \mathcal{Q}'(\mathcal{C})$. We first prove this assertion for the case where \mathcal{G}' is constructed from \mathcal{G} by merging only a single pair of constraint nodes, $j_1, j_2 \in \mathcal{J}$,

of \mathcal{G} . In this case, by the assumption of the proposition, there are two possibilities.

- 1) There is no overlap between the variable nodes that are connected to j_1 and the variable nodes that are connected to j_2 . Denote by \mathbf{c}_1 and \mathbf{c}_2 the sub-codewords associated with the variable nodes connected to j_1 and j_2 respectively. In this case there is no overlap between \mathbf{c}_1 and \mathbf{c}_2 . This case is illustrated in Figure 2.
- 2) Exactly one variable node is connected to both j_1 and j_2 , that is there is an overlap of one bit, $c_{1,2}$, between \mathbf{c}_1 and \mathbf{c}_2 . This case is illustrated in Figure 3.

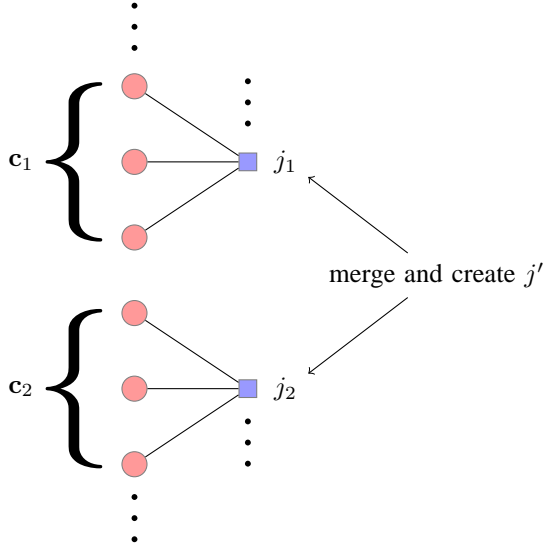


Fig. 2. Merging two parity nodes, j_1 and j_2 , in the Tanner graph of the code \mathcal{C} . In this case there is no overlap between \mathbf{c}_1 and \mathbf{c}_2 .

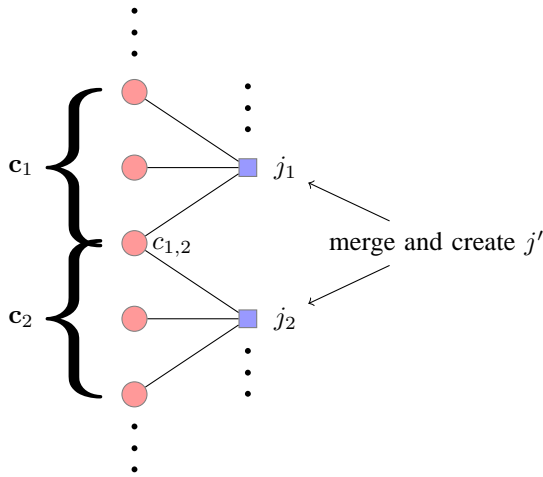


Fig. 3. Merging two parity nodes, j_1 and j_2 , in the Tanner graph of the code \mathcal{C} . In this case there is an overlap of one bit, $c_{1,2}$, between \mathbf{c}_1 and \mathbf{c}_2 .

Now consider the first case (Figure 2). Suppose that $\mathbf{c} \in \mathcal{Q}(\mathcal{C})$. Then for $j = j_1, j_2$ there exists a set of weights $\{w_{j,\mathbf{g}} \geq$

$0\}$ for $\mathbf{g} \in \mathcal{C}_j$ such that

$$\sum_{\mathbf{g} \in \mathcal{C}_j} w_{j,\mathbf{g}} = 1$$

and

$$c_i = \sum_{\mathbf{g} \in \mathcal{C}_j, g_i=1} w_{j,\mathbf{g}} \quad \forall i \in \mathcal{N}_j$$

Define the set $\{w_{j',\mathbf{g}}\}$ for $\mathbf{g} = (\mathbf{g}_1, \mathbf{g}_2)$, where \mathbf{g}_1 and \mathbf{g}_2 correspond to the sub-codewords \mathbf{c}_1 and \mathbf{c}_2 respectively in Figure 2, by

$$w_{j',(\mathbf{g}_1, \mathbf{g}_2)} \triangleq w_{j_1, \mathbf{g}_1} \cdot w_{j_2, \mathbf{g}_2}$$

It follows from this definition that $w_{j',(\mathbf{g}_1, \mathbf{g}_2)} \geq 0$, and

$$\sum_{\mathbf{g} \in \mathcal{C}'_j} w_{j',\mathbf{g}} = \sum_{\mathbf{g}_1 \in \mathcal{C}_{j_1}} \sum_{\mathbf{g}_2 \in \mathcal{C}_{j_2}} w_{j_1, \mathbf{g}_1} w_{j_2, \mathbf{g}_2} = 1$$

Furthermore, for $i \in \mathcal{N}_{j_1}$

$$\begin{aligned} \sum_{\substack{\mathbf{g} \in \mathcal{C}'_j \\ g_i=1}} w_{j',\mathbf{g}} &= \sum_{\substack{(\mathbf{g}_1, \mathbf{g}_2) \in \mathcal{C}'_j \\ g_{1,i}=1}} w_{j',(\mathbf{g}_1, \mathbf{g}_2)} \\ &= \sum_{\substack{\mathbf{g}_1 \in \mathcal{C}_{j_1} \\ g_{1,i}=1}} w_{j_1, \mathbf{g}_1} \sum_{\mathbf{g}_2 \in \mathcal{C}_{j_2}} w_{j_2, \mathbf{g}_2} = c_i \end{aligned}$$

where $g_{1,i}$ ($g_{2,i}$, respectively) is the i 'th component of \mathbf{g}_1 (\mathbf{g}_2). Similarly, for $i \in \mathcal{N}_{j_2}$

$$\sum_{\mathbf{g} \in \mathcal{C}'_j, g_i=1} w_{j',\mathbf{g}} = c_i$$

This shows that in the case considered $\mathbf{c} \in \mathcal{Q}'(\mathcal{C})$.

Next consider the second case (Figure 3). Suppose that $\mathbf{c} \in \mathcal{Q}(\mathcal{C})$. Then for $j = j_1, j_2$ there exists a set of weights $\{w_{j,\mathbf{g}} \geq 0\}$ for $\mathbf{g} \in \mathcal{C}_j$ such that

$$\sum_{\mathbf{g} \in \mathcal{C}_j} w_{j,\mathbf{g}} = 1 \quad (32)$$

and

$$c_i = \sum_{\mathbf{g} \in \mathcal{C}_j, g_i=1} w_{j,\mathbf{g}} \quad \forall i \in \mathcal{N}_j \quad (33)$$

Let $\hat{\mathbf{c}}_1$ denote the sub-codeword \mathbf{c}_1 excluding the common bit $c_{1,2}$. Similarly $\hat{\mathbf{c}}_2$ is the sub-codeword \mathbf{c}_2 excluding $c_{1,2}$. Define the set $\{w_{j',\mathbf{g}}\}$ for $\mathbf{g} = (\hat{\mathbf{g}}_1, g_{1,2}, \hat{\mathbf{g}}_2)$, where $\hat{\mathbf{g}}_1$, $g_{1,2}$ and $\hat{\mathbf{g}}_2$ correspond to $\hat{\mathbf{c}}_1$, $c_{1,2}$ and $\hat{\mathbf{c}}_2$ respectively, by

$$w_{j',\mathbf{g}} = w_{j',(\hat{\mathbf{g}}_1, g_{1,2}, \hat{\mathbf{g}}_2)} \triangleq \begin{cases} w_{j_1,(\hat{\mathbf{g}}_1, 1)} \cdot w_{j_2,(1, \hat{\mathbf{g}}_2)} / c_{1,2} & \text{if } g_{1,2} = 1 \\ w_{j_1,(\hat{\mathbf{g}}_1, 0)} \cdot w_{j_2,(0, \hat{\mathbf{g}}_2)} / (1 - c_{1,2}) & \text{if } g_{1,2} = 0 \end{cases}$$

It follows from this definition that $w_{j',\mathbf{g}} \geq 0$, and

$$\begin{aligned} \sum_{\mathbf{g} \in \mathcal{C}'_j} w_{j',\mathbf{g}} &= \frac{1}{1 - c_{1,2}} \sum_{\hat{\mathbf{g}}_1 : (\hat{\mathbf{g}}_1, 0) \in \mathcal{C}_{j_1}} \sum_{\hat{\mathbf{g}}_2 : (0, \hat{\mathbf{g}}_2) \in \mathcal{C}_{j_2}} w_{j_1,(\hat{\mathbf{g}}_1, 0)} w_{j_2,(0, \hat{\mathbf{g}}_2)} \\ &\quad + \frac{1}{c_{1,2}} \sum_{\hat{\mathbf{g}}_1 : (\hat{\mathbf{g}}_1, 1) \in \mathcal{C}_{j_1}} \sum_{\hat{\mathbf{g}}_2 : (1, \hat{\mathbf{g}}_2) \in \mathcal{C}_{j_2}} w_{j_1,(\hat{\mathbf{g}}_1, 1)} w_{j_2,(1, \hat{\mathbf{g}}_2)} \\ &= 1 \end{aligned}$$

where the last equality follows from the following equalities, which are implied by (32) and (33),

$$c_{1,2} = \sum_{\hat{\mathbf{g}}_1 : (\hat{\mathbf{g}}_1, 1) \in \mathcal{C}_{j_1}} w_{j_1, (\hat{\mathbf{g}}_1, 1)} = \sum_{\hat{\mathbf{g}}_2 : (1, \hat{\mathbf{g}}_2) \in \mathcal{C}_{j_2}} w_{j_2, (1, \hat{\mathbf{g}}_2)} \quad (34)$$

$$1 - c_{1,2} = \sum_{\hat{\mathbf{g}}_1 : (\hat{\mathbf{g}}_1, 0) \in \mathcal{C}_{j_1}} w_{j_1, (\hat{\mathbf{g}}_1, 0)} = \sum_{\hat{\mathbf{g}}_2 : (0, \hat{\mathbf{g}}_2) \in \mathcal{C}_{j_2}} w_{j_2, (0, \hat{\mathbf{g}}_2)} \quad (35)$$

It remains to show that

$$\sum_{\mathbf{g} \in \mathcal{C}'_j, g_i=1} w_{j', \mathbf{g}} = c_i \quad (36)$$

This is shown by considering the following three possibilities for i : $i \in \mathcal{N}_{j_1} \cap \mathcal{N}_{j_2}$, $i \in \mathcal{N}_{j_1} \setminus \mathcal{N}_{j_2}$ and $i \in \mathcal{N}_{j_2} \setminus \mathcal{N}_{j_1}$. In the first case, $i \in \mathcal{N}_{j_1} \cap \mathcal{N}_{j_2}$, we have $c_i = c_{1,2}$. In this case

$$\begin{aligned} \sum_{\substack{\mathbf{g} \in \mathcal{C}'_j \\ g_i=1}} w_{j', \mathbf{g}} &= \sum_{(\hat{\mathbf{g}}_1, 1, \hat{\mathbf{g}}_2) \in \mathcal{C}'_j} \frac{1}{c_{1,2}} w_{j_1, (\hat{\mathbf{g}}_1, 1)} \cdot w_{j_2, (1, \hat{\mathbf{g}}_2)} \\ &= \frac{1}{c_{1,2}} \sum_{\hat{\mathbf{g}}_1 : (\hat{\mathbf{g}}_1, 1) \in \mathcal{C}_{j_1}} w_{j_1, (\hat{\mathbf{g}}_1, 1)} \sum_{\hat{\mathbf{g}}_2 : (1, \hat{\mathbf{g}}_2) \in \mathcal{C}_{j_2}} w_{j_2, (1, \hat{\mathbf{g}}_2)} \\ &= c_{1,2} \end{aligned}$$

where the last equality follows from (34).

In the second case, $i \in \mathcal{N}_{j_1} \setminus \mathcal{N}_{j_2}$, we have

$$\begin{aligned} \sum_{\substack{\mathbf{g} \in \mathcal{C}'_j \\ g_i=1}} w_{j', \mathbf{g}} &= \sum_{\substack{(\hat{\mathbf{g}}_1, 1, \hat{\mathbf{g}}_2) \in \mathcal{C}'_j \\ g_{1,i}=1}} \frac{w_{j_1, (\hat{\mathbf{g}}_1, 1)} \cdot w_{j_2, (1, \hat{\mathbf{g}}_2)}}{c_{1,2}} \\ &+ \sum_{\substack{(\hat{\mathbf{g}}_1, 0, \hat{\mathbf{g}}_2) \in \mathcal{C}'_j \\ g_{1,i}=1}} \frac{w_{j_1, (\hat{\mathbf{g}}_1, 0)} \cdot w_{j_2, (0, \hat{\mathbf{g}}_2)}}{1 - c_{1,2}} \\ &= \sum_{\substack{\hat{\mathbf{g}}_1 : (\hat{\mathbf{g}}_1, 1) \in \mathcal{C}_{j_1} \\ g_{1,i}=1}} \frac{w_{j_1, (\hat{\mathbf{g}}_1, 1)}}{c_{1,2}} \sum_{\hat{\mathbf{g}}_2 : (1, \hat{\mathbf{g}}_2) \in \mathcal{C}_{j_2}} w_{j_2, (1, \hat{\mathbf{g}}_2)} \\ &+ \sum_{\substack{\hat{\mathbf{g}}_1 : (\hat{\mathbf{g}}_1, 0) \in \mathcal{C}_{j_1} \\ g_{1,i}=1}} \frac{w_{j_1, (\hat{\mathbf{g}}_1, 0)}}{1 - c_{1,2}} \sum_{\hat{\mathbf{g}}_2 : (0, \hat{\mathbf{g}}_2) \in \mathcal{C}_{j_2}} w_{j_2, (0, \hat{\mathbf{g}}_2)} \\ &= \sum_{\substack{\hat{\mathbf{g}}_1 : (\hat{\mathbf{g}}_1, 1) \in \mathcal{C}_{j_1} \\ g_{1,i}=1}} w_{j_1, (\hat{\mathbf{g}}_1, 1)} + \sum_{\substack{\hat{\mathbf{g}}_1 : (\hat{\mathbf{g}}_1, 0) \in \mathcal{C}_{j_1} \\ g_{1,i}=1}} w_{j_1, (\hat{\mathbf{g}}_1, 0)} \\ &= c_i \end{aligned}$$

where the third equality is due to (34) and (35), and the fourth equality is due to (33) (with $j = j_1$). The proof that (36) holds in the third case, $i \in \mathcal{N}_{j_2} \setminus \mathcal{N}_{j_1}$, is identical. Thus in all three cases considered (36) holds, and we conclude that $\mathbf{c} \in \mathcal{Q}'(\mathcal{C})$ as claimed.

We thus conclude that when we merge a single pair of constraint nodes, $\mathcal{Q}(\mathcal{C}) = \mathcal{Q}'(\mathcal{C})$. We proceed to prove that this holds for a general merge up of a set of constraint nodes $V = \{j_1, \dots, j_r\}$, for which the subgraph of \mathcal{G} induced by the nodes in V and their direct neighbors is cycle free, into one node j' . We denote the new graph by \mathcal{G}' . We start from the original graph \mathcal{G} with the corresponding polytope $\mathcal{Q}(\mathcal{C}) = \mathcal{Q}^{(1)}(\mathcal{C})$, and select a constraint node $\tilde{j} \in V$ arbitrarily. Now we select

a node to merge with node \tilde{j} . If there exists some node $\tilde{j}' \in V$ such that $\mathcal{N}_{\tilde{j}} \cap \mathcal{N}_{\tilde{j}'} \neq \emptyset$ then \tilde{j}' is selected to be merged with \tilde{j} . Otherwise, $\tilde{j}' \in V$ is picked arbitrarily. Now \tilde{j} and \tilde{j}' are merged into a new constraint node $\tilde{j}^{(1)}$. After performing the merging operation on these two nodes, a new graph $\mathcal{G}^{(2)}$ is formed with the corresponding polytope, $\mathcal{Q}^{(2)}(\mathcal{C})$. Now, in \mathcal{G} , the two constraint nodes selected for merging either have no common variable node or are connected to a single common variable node. By what we have already shown, we know that $\mathcal{Q}^{(1)}(\mathcal{C}) = \mathcal{Q}^{(2)}(\mathcal{C})$. Now we repeat the process. If there is a node \tilde{j}'' within the remaining nodes in V such that $\mathcal{N}_{\tilde{j}^{(1)}} \cap \mathcal{N}_{\tilde{j}''} \neq \emptyset$ then \tilde{j}'' is selected to be merged with $\tilde{j}^{(1)}$, otherwise \tilde{j}'' is selected arbitrarily. Once \tilde{j}'' is chosen, it is merged with $\tilde{j}^{(1)}$ into a new constraint node $\tilde{j}^{(2)}$, forming a new graph $\mathcal{G}^{(3)}$ with its corresponding polytope, $\mathcal{Q}^{(3)}(\mathcal{C})$. By this selection process, in $\mathcal{G}^{(2)}$, the two constraint nodes selected for merging again have either no common variable node or are connected to a single common variable node, and thus $\mathcal{Q}^{(2)}(\mathcal{C}) = \mathcal{Q}^{(3)}(\mathcal{C})$. This merge up process continues until we have created the graph $\mathcal{G}' = \mathcal{G}^{(r)}$ with polytope $\mathcal{Q}'(\mathcal{C}) = \mathcal{Q}^{(r)}(\mathcal{C})$. Thus we have shown that,

$$\mathcal{Q}(\mathcal{C}) = \mathcal{Q}^{(1)}(\mathcal{C}) = \mathcal{Q}^{(2)}(\mathcal{C}) = \dots = \mathcal{Q}^{(r)}(\mathcal{C}) = \mathcal{Q}'(\mathcal{C})$$

The proof of the general case, where we merge several non-overlapping groups of variable nodes in \mathcal{G} in order to form \mathcal{G}' (e.g., in the example shown in Figure 1, where we merge j_1 and j_2 into j'_1 , and j_3 and j_4 into j'_2), now follows immediately. Thus we have shown that $\mathcal{Q}(\mathcal{C}) = \mathcal{Q}'(\mathcal{C})$. This implies that $P_e(\mathbf{c}) = P'_e(\mathbf{c})$. \square

Proposition 3 implies the following. Consider some graphical representation \mathcal{G} of a code \mathcal{C} and suppose that we wish to obtain a new graphical representation \mathcal{G}' by merging constraint nodes such that when using LP decoding, the error probability of \mathcal{G}' is smaller than the error probability of \mathcal{G} . Then, when considering candidate constraint nodes for merge up, it is sufficient to consider only constraint nodes j_1, \dots, j_r such that the subgraph of \mathcal{G} induced by j_1, \dots, j_r and their direct neighbors contains a cycle.

In the sequel, we will use a variant of Proposition 3, where upon merging nodes j_1, j_2, \dots, j_r into j' , we keep the original nodes j_1, j_2, \dots, j_r as well as the new node j' (the reason for this is that we want to enable some of the nodes j_1, j_2, \dots, j_r to be merged with other nodes). Due to Propositions 1 and 3, keeping j_1, j_2, \dots, j_r has no effect on the resulting $\mathcal{Q}'(\mathcal{C})$ and $P'_e(\mathbf{c})$.

V. BOUND ON THE MINIMUM AND FRACTIONAL DISTANCE OF SPECIFIC CODES

It was already shown in [1] that LP decoding can be used to obtain the fractional distance, which is also a lower bound on the minimum distance of specific linear codes, in polynomial time complexity. In this section, we show how Algorithm 1 can be used to obtain a lower bound on the minimum distance of a given code, and that this bound is also an upper bound on the fractional distance. Assuming the degree of the check nodes is bounded by a constant independent of N , this

procedure requires execution of Algorithm 1 a number of times proportional to N , and thus the total complexity is $O(N^2)$.

Let $r \in \mathcal{J}$ be a check node and let \mathbf{c}_r be some nonzero local codeword of r . The idea is to search for a minimum-weight vector subject to the constraint that \mathbf{c}_r is the local codeword on node r (later we will show how such vectors allow to obtain a lower bound on the minimum distance). This conforms to the setting of Problem-P, if we set $\gamma_i = 1$ for all i . Denote $\mathcal{I}_r \triangleq \mathcal{I} \setminus \mathcal{N}_r$ and $\mathcal{J}_r \triangleq \mathcal{J} \setminus \{r\}$. We would like to obtain the solution by running Algorithm 1 on a modified version of the graph in which we remove the node r , all its neighbors \mathcal{N}_r and the edges connected to these neighbors. However, in order to maintain a correct representation of the code, we must account for the specific nonzero local codeword \mathbf{c}_r . To do this, we look at all constraint nodes $j \in \mathcal{J}_r$ where $\mathcal{N}_j \cap \mathcal{N}_r \neq \emptyset$. Let $j \in \mathcal{J}_r$ be such a constraint node described by a matrix H_j with columns $\{\mathbf{h}_i\}_{i \in \mathcal{N}_j}$; this situation is exemplified in Figure 4(a). Since we will be forcing the variables in $\mathcal{N}_j \cap \mathcal{N}_r$ to a value depending on \mathbf{c}_r , we have that the local codeword vector $\mathbf{c}_j \in \mathcal{C}_j$ on node j satisfies

$$\sum_{i \in \mathcal{N}_j \setminus \mathcal{N}_r} c_i \mathbf{h}_i = \sum_{i \in \mathcal{N}_j \cap \mathcal{N}_r} c_i \mathbf{h}_i \triangleq \tilde{\mathbf{h}}_j^{r, \mathbf{c}_r} \quad (37)$$

We now remove parity check r and all its neighbors from the graph. Consequently, in the remaining graph we observe that check node j describes a coset code where a standard constraint of the form $H_j \mathbf{c}_j = 0$ is replaced by the constraint $H_j^r \mathbf{c}_j^r = \tilde{\mathbf{h}}_j^{r, \mathbf{c}_r}$, where $H_j^r = \{\mathbf{h}_i\}_{i \in \mathcal{N}_j \setminus \mathcal{N}_r}$ and $\mathbf{c}_j^r = \{c_i\}_{i \in \mathcal{N}_j \setminus \mathcal{N}_r}$. This is exemplified in Figure 4(b). Denote the set of local codewords of this coset code by $\mathcal{C}_j^{r, \mathbf{c}_r}$. Also denote $\mathbf{c}^{(r)} = \{c_i\}_{i \in \mathcal{I}_r}$, $\omega^{(r)} = \{\omega_{j, \mathbf{g}}\}_{j \in \mathcal{J}_r, \mathbf{g} \in \mathcal{C}_j^{r, \mathbf{c}_r}}$. Problem- $\mathbf{P}^{r, \mathbf{c}_r}$ is defined as follows.

$$\min_{\mathbf{c}^{(r)}, \omega^{(r)}} \sum_{i \in \mathcal{I}_r} c_i \quad (38)$$

subject to

$$w_{j, \mathbf{g}} \geq 0 \quad \forall j \in \mathcal{J}_r, \mathbf{g} \in \mathcal{C}_j^{r, \mathbf{c}_r} \quad (39)$$

$$\sum_{\mathbf{g} \in \mathcal{C}_j^{r, \mathbf{c}_r}} w_{j, \mathbf{g}} = 1 \quad \forall j \in \mathcal{J}_r \quad (40)$$

$$c_i = \sum_{\mathbf{g} \in \mathcal{C}_j^{r, \mathbf{c}_r}, g_i = 1} w_{j, \mathbf{g}} \quad \forall j \in \mathcal{J}_r, i \in \mathcal{N}_j \setminus \mathcal{N}_r. \quad (41)$$

Thus, by setting $\gamma_i = 1 \forall i \in \mathcal{I}$, Problem- $\mathbf{P}^{r, \mathbf{c}_r}$ is easily seen to be an instance of Problem-P, and thus its solution can be approximated arbitrarily closely by Algorithm 1 in linear time. The only modification we need to make is to account for the coset codes $\{\mathcal{C}_j^{r, \mathbf{c}_r}\}$, and this can be accomplished by replacing the definition of $A_{k, j}$ and $B_{k, j}$ in (15) by

$$\begin{aligned} A_{k, j} &\triangleq \sum_{\mathbf{g} \in \mathcal{C}_j^{r, \mathbf{c}_r}, g_k = 1} e^{-K \sum_{i \in \mathcal{N}_j \setminus (\mathcal{N}_r \cup \{k\})} u_{i, j} g_i} \\ B_{k, j} &\triangleq \sum_{\mathbf{g} \in \mathcal{C}_j^{r, \mathbf{c}_r}, g_k = 0} e^{-K \sum_{i \in \mathcal{N}_j \setminus (\mathcal{N}_r \cup \{k\})} u_{i, j} g_i} \end{aligned} \quad (42)$$

These can be computed efficiently for any coset code $\mathcal{C}_j^{r, \mathbf{c}_r}$ using the method described in Section III-A. However, instead

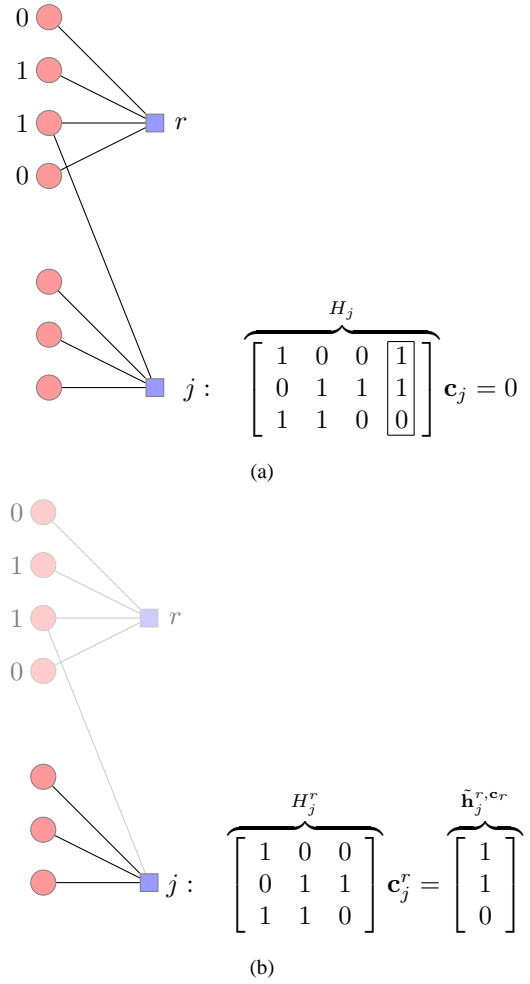


Fig. 4. Coset codes formed when a codeword $\mathbf{c}_r = (0, 1, 1, 0)$ is forced on constraint node r which is removed. (a) The rightmost column of H_j corresponds to a removed variable node forced to a '1' value. (b) The new code $\mathcal{C}_j^{r, \mathbf{c}_r}$ is formed as r and \mathcal{N}_r are removed from the graph.

of (20) we now have (note that for simplicity we omit the dependence on j)

$$\begin{aligned} A_k &\triangleq \sum_{\mathbf{g} : H^r \mathbf{g} = \tilde{\mathbf{h}}^{r, \mathbf{c}_r}, g_k = 1} e^{-K \left(\sum_{i=0}^{n-1} u_i g_i - u_k \right)} \\ B_k &\triangleq \sum_{\mathbf{g} : H^r \mathbf{g} = \tilde{\mathbf{h}}^{r, \mathbf{c}_r}, g_k = 0} e^{-K \sum_{i=0}^{n-1} u_i g_i}. \end{aligned} \quad (43)$$

It can be seen that the only alteration we need to make is to replace (28) and (29) by

$$A_k = e^{K u_k} \sum_{\mathbf{s}} E(k, \mathbf{s}, 1) \tilde{E}(k, \mathbf{s} \oplus \tilde{\mathbf{h}}^{r, \mathbf{c}_r}) \quad (44)$$

and

$$B_k = \sum_{\mathbf{s}} E(k, \mathbf{s}, 0) \tilde{E}(k, \mathbf{s} \oplus \tilde{\mathbf{h}}^{r, \mathbf{c}_r}) \quad (45)$$

for $k = 0, \dots, n-1$. For the calculation of $D(\mathbf{u})$ of a coset code, we can appropriately modify and use the efficient method from Section III-B. The necessary modification for a coset code characterized by a vector $\tilde{\mathbf{h}}^{r, \mathbf{c}_r}$, is that we need to

recursively calculate

$$A(n-1, \tilde{\mathbf{h}}^{r, \mathbf{c}_r}) \quad (46)$$

rather than $A(n-1, 0)$.

Solving Problem- P^{r, \mathbf{c}_r} thus finds an approximate minimum-weight vector $\hat{\mathbf{c}}$ subject to enforcing a local codeword on parity check r . We repeatedly apply this method, solving Problem- P^{r, \mathbf{c}_r} over all nonzero local codewords $\mathbf{c}_r \in \mathcal{C}_r \setminus \{\mathbf{0}_r\}$, and for each local codeword we record both a lower bound $\underline{l}_{\mathbf{c}_r}^r = D(\mathbf{u})$ and an upper bound $\overline{l}_{\mathbf{c}_r}^r = P(\tilde{\lambda})$ (see (18)) on the optimal value. In this manner, we create two sets of values $\{\underline{l}_{\mathbf{c}_r}^r\}_{\mathbf{c}_r \in \mathcal{C}_r \setminus \{\mathbf{0}_r\}}$ and $\{\overline{l}_{\mathbf{c}_r}^r\}_{\mathbf{c}_r \in \mathcal{C}_r \setminus \{\mathbf{0}_r\}}$. Next, we calculate the minima

$$\underline{l}_{\min}^r \triangleq \min_{\mathbf{c}_r \in \mathcal{C}_r \setminus \{\mathbf{0}_r\}} \underline{l}_{\mathbf{c}_r}^r \quad (47)$$

and

$$\overline{l}_{\min}^r \triangleq \min_{\mathbf{c}_r \in \mathcal{C}_r \setminus \{\mathbf{0}_r\}} \overline{l}_{\mathbf{c}_r}^r \quad (48)$$

Finally, the entire procedure is repeated for all $r \in \mathcal{J}$ and we calculate

$$\underline{l}_{\min} \triangleq \min_{r \in \mathcal{J}} \{\underline{l}_{\min}^r\}, \quad \overline{l}_{\min} \triangleq \min_{r \in \mathcal{J}} \{\overline{l}_{\min}^r\} \quad (49)$$

We refer to this process as *Algorithm 2*, which is summarized in what follows.

Algorithm 2: Given a GLDPC code, do:

- **loop over** $r \in \mathcal{J}$
 - **loop over** $\mathbf{c}_r \in \mathcal{C}_r \setminus \{\mathbf{0}_r\}$
 - * **loop over** $i \in \mathcal{N}_r$ **and** $j \in \mathcal{N}_i$
 - Compute $\tilde{\mathbf{h}}_j^{r, \mathbf{c}_r}$ using (37)
 - Define $H_j^r = \{\mathbf{h}_i\}_{i \in \mathcal{N}_j \setminus \mathcal{N}_r}$
 - Compute all codewords of the local coset code $\mathcal{C}_j^{r, \mathbf{c}_r}$ defined by $H_j^r \tilde{\mathbf{c}}_r = \tilde{\mathbf{h}}_j^{r, \mathbf{c}_r}$
 - * Run Algorithm 1 to solve Problem- P^{r, \mathbf{c}_r} , defined by (38)-(41). While running the algorithm, use the definitions of $A_{k,j}$ and $B_{k,j}$ in (42) instead of those in (15)
 - * Set $\underline{l}_{\mathbf{c}_r}^r = D(\mathbf{u})$ and $\overline{l}_{\mathbf{c}_r}^r = P(\tilde{\lambda})$ where the vectors \mathbf{u} and $\tilde{\lambda}$ are output by Algorithm 1. Calculate $D(\mathbf{u})$ using (10) or by the more efficient method in Section III-B, with (46) instead of (30).
 - Calculate $\underline{l}_{\min}^r = \min_{\mathbf{c}_r \in \mathcal{C}_r \setminus \{\mathbf{0}_r\}} \underline{l}_{\mathbf{c}_r}^r$ and $\overline{l}_{\min}^r = \min_{\mathbf{c}_r \in \mathcal{C}_r \setminus \{\mathbf{0}_r\}} \overline{l}_{\mathbf{c}_r}^r$
- Output $\underline{l}_{\min} = \min_{r \in \mathcal{J}} \{\underline{l}_{\min}^r\}$ and $\overline{l}_{\min} = \min_{r \in \mathcal{J}} \{\overline{l}_{\min}^r\}$

Proposition 4: \underline{l}_{\min} , output by Algorithm 2, is a lower bound on the minimum distance of the code.

Proof: First, we claim that \underline{l}_{\min}^r , defined in (47), is a lower bound on the minimum distance of the code, subject to the restriction that the local codeword on node r is nonzero. This is due to the fact that a minimum-distance codeword $\tilde{\mathbf{c}}^r$ subject to this restriction must have some nonzero local codeword \mathbf{c}_r on check node r , and while running Algorithm 1 with the values of \mathbf{c}_r forced on variable nodes \mathcal{N}_r , we optimize over a set containing $\tilde{\mathbf{c}}^r$. Furthermore, due to weak duality, the result $\underline{l}_{\mathbf{c}_r}^r = D(\mathbf{u})$ is a lower bound on the optimal value. Consequently, \underline{l}_{\min}^r is a lower bound on the minimum distance subject to the above restriction. Now, since a (global)

minimum-distance codeword $\tilde{\mathbf{c}}$ must contain a check node r' , the neighbors of which represent a nonzero local codeword $\mathbf{c}_{r'}$, then at some point Algorithm 2 will have passed through node r' and the local codeword $\mathbf{c}_{r'}$ and produced a lower bound on the weight of $\tilde{\mathbf{c}}$. Since we take the minimum value in (47) and (49), \underline{l}_{\min} is a lower bound on the minimum distance of the code. ■

Recall that we assume parity check degrees which do not depend on N . Consequently, for any check node r , the bounds \underline{l}_{\min}^r and \overline{l}_{\min}^r are obtained by running Algorithm 1 a constant number of times. Repeating this process over all check nodes thus entails a total complexity of $O(N^2)$.

Next, we claim that \overline{l}_{\min} is at least as large as the fractional distance.

Proposition 5: The bound \overline{l}_{\min} output by Algorithm 2 is an upper bound on the fractional distance of the code.

Proof: Recall that \overline{l}_{\min} was obtained by running Algorithm 1 over some reduced version of the code, corresponding to the selection of a nonzero local codeword \mathbf{c}_r on some check node r . That is, we find the minimum of $\sum_{i \in \mathcal{I}} c_i$ over the original LP polytope $\mathcal{Q}(\mathcal{C})$ while also imposing the values \mathbf{c}_r of the local codeword. For $\mathbf{c}_r = \{c_{r,i}\}_{i \in \mathcal{N}_r}$, let $\mathcal{Q}_{\mathbf{c}_r}(\mathcal{C}) = \{(p_1, \dots, p_N) \in \mathcal{Q}(\mathcal{C}) : \forall i \in \mathcal{N}_r, p_i = c_{r,i}\}$ be the polytope $\mathcal{Q}(\mathcal{C})$ with the added restriction of the local codeword \mathbf{c}_r . Now, the minimum of any LP is attained at a vertex. Consequently, if we show that $\mathcal{V}(\mathcal{Q}_{\mathbf{c}_r}(\mathcal{C})) \subseteq \mathcal{V}(\mathcal{Q}(\mathcal{C}))$, where $\mathcal{V}(\mathcal{P})$ is the vertex set of the polytope \mathcal{P} , then the value of \overline{l}_{\min} output by Algorithm 2 is an upper bound on the L_1 -norm of a nonzero pseudocodeword in \mathcal{C} , and is thus an upper bound on the fractional distance. To this end, it will suffice to show that imposing an integer value on a single coordinate does not create new vertices. Without loss of generality, let $\mathcal{Q}^N(\mathcal{C}) \triangleq \mathcal{Q}(\mathcal{C}) \cap \{c_N = 1\}$, and $\mathbf{v} \in \mathcal{V}(\mathcal{Q}^N(\mathcal{C}))$. We now show that $\mathbf{v} \in \mathcal{V}(\mathcal{Q}(\mathcal{C}))$. In essence, an easy algebraic argument will be used. First, note that $\mathcal{Q}(\mathcal{C})$ can be represented as a matrix inequality

$$A\mathbf{c} \succeq \mathbf{b} \quad (50)$$

where \mathbf{c} and \mathbf{b} are column vectors, A is a matrix representing, together with \mathbf{b} , the constraints (8)¹ for all $j \in \mathcal{J}$, and \succeq is the standard coordinate-wise inequality. The polytope $\mathcal{Q}^N(\mathcal{C})$ can be similarly represented by

$$A'\mathbf{c} \succeq \mathbf{b}'$$

where

$$A' = \begin{bmatrix} A \\ 0 \ 0 \ \dots \ 0 \ 1 \end{bmatrix}, \quad \mathbf{b}' = \begin{bmatrix} \mathbf{b} \\ 1 \end{bmatrix}$$

We make use of the property that a vertex is the intersection of N independent hyperplanes. Specifically, if $\mathbf{v} \in \mathcal{Q}^N(\mathcal{C})$ then $\mathbf{v} \in \mathcal{V}(\mathcal{Q}^N(\mathcal{C}))$ if and only if there exists a subset of N rows A'_1 of A' , and a corresponding subvector \mathbf{b}'_1 of \mathbf{b}' such that

¹The constraints (8), which are valid for plain LDPC codes, are clearly expressible in matrix form. In Section VII we will see that for GLDPC codes, the fundamental polytope is also expressible in the form (50), and thus the conclusion of Proposition 5 holds also for GLDPC codes.

$$A'_1 \mathbf{c} = \mathbf{b}'_1$$

and $\det(A'_1) \neq 0$ (see, e.g., [13, p. 185]). Suppose $\mathbf{v} \in \mathcal{V}(\mathcal{Q}^N(\mathcal{C}))$. If the matrix A'_1 does not contain the last row of A' , then it is also a sub-matrix of A and we conclude that $\mathbf{v} \in \mathcal{V}(\mathcal{Q}(\mathcal{C}))$, as required. If A'_1 contains the last row of A' , then we replace this row in A'_1 with

$$[0 \ 0 \ \dots \ 0 \ -1] \quad (51)$$

which appears in A due to the constraint $c_N \leq 1$ (see (8)); with this replacement the determinant is still nonzero and we conclude that $\mathbf{v} \in \mathcal{Q}(\mathcal{C})$ is the intersection of N independent hyperplanes of $\mathcal{Q}(\mathcal{C})$, and thus $\mathbf{v} \in \mathcal{V}(\mathcal{Q}(\mathcal{C}))$. ■

Discussion. In this section it was shown that \underline{l}_{\min} and \overline{l}_{\min} , output by Algorithm 2 and obtained with complexity $O(N^2)$, constitute a lower bound on the overall minimum distance and an upper bound on the fractional distance, respectively. Due to (19) and the proof of [8, Theorem 1], it can be seen that $\overline{l}_{\min} - \underline{l}_{\min} \leq \delta N$ where $\delta > 0$ can be made as small as desired. Moreover, it is possible to improve the lower bound on the minimum distance in the following two ways. First, the node merging technique presented in Section IV can be used to produce a tighter LP relaxation, and thus a better lower bound on the minimum distance. This approach is exemplified in Section VIII. Second, instead of examining single constraint nodes on which a local codeword is forced, one could divide \mathcal{J} into pairs of constraint nodes, and for each pair examine all nonzero combinations of their local codewords. For each such nonzero combination of pairs of codewords, it is possible to find a minimum-weight vector subject to forcing the variable node neighbors to values corresponding to these codewords, similar to what is done in Algorithm 2. As another possible variant to Algorithm 2, we propose the following greedy procedure, which we term the *bar method*.

We set a target level or “bar”, denoted BAR, for the lower bound which the procedure attempts to exceed, as follows. We loop over all check nodes, as in Algorithm 2. For each check node $r \in \mathcal{J}$ we evaluate \underline{l}_{\min}^r , defined in (47). If $\underline{l}_{\min}^r \geq \text{BAR}$, we proceed to the next check node. If $\underline{l}_{\min}^r < \text{BAR}$, say due to a local codeword \mathbf{c}_r^0 for which $\underline{l}_{\mathbf{c}_r^0} < \text{BAR}$, we refine the bound $\underline{l}_{\mathbf{c}_r^0}$ as follows. First we pick a check node $j \in \mathcal{N}_i$ for some $i \in \mathcal{N}_r$; thus j is a check node at distance 2 from r , with respect to \mathcal{G} . Next we loop over the local codewords $\{\mathbf{c}_j\}$ on node j which coincide with \mathbf{c}_r^0 (i.e., which have the same values on the variable nodes in $\mathcal{N}_j \cap \mathcal{N}_r$). For each such local codeword, we run Algorithm 1, forcing local codewords on *both* check nodes r and j . This forcing of local codewords jointly on a pair of check nodes produces a lower bound $\underline{l}_{\mathbf{c}_r^0, \mathbf{c}_j}$ on the minimum distance subject to forcing both check nodes to these local codewords. Define $\underline{l}_{\min}^{r,j} \triangleq \min_{\mathbf{c}_j \in \mathcal{C}_j} \{\underline{l}_{\mathbf{c}_r^0, \mathbf{c}_j} : \mathbf{c}_j \text{ coincides with } \mathbf{c}_r^0\}$. If $\underline{l}_{\min}^{r,j} \geq \text{BAR}$, we conclude that the bar has been exceeded for check node r , and proceed to the next check node. Otherwise, we pick another check node $j \in \mathcal{N}_i$ for some $i \in \mathcal{N}_r$ and repeat the process until for some choice of node j at distance 2 from r the bar is exceeded. If the bar is not exceeded for all nodes j at distance 2 from r , the

procedure is terminated with failure. If, on the other hand, for all $r \in \mathcal{J}$ we have $\underline{l}_{\min}^r \geq \text{BAR}$ or otherwise if for all $\mathbf{c}_r^0 \in \mathcal{C}_r$ we have $\underline{l}_{\min}^{r,j} \geq \text{BAR}$ for some node j at distance 2 from r , then we say that the level BAR is *attainable*. Due to the bound refining process, an attainable bar level is guaranteed to be a lower bound on the minimum distance. Using initial lower and upper values for the bar (which can be determined ad-hoc), we can run the procedure, each time using a different level for the bar, and use the bisection method to find the highest attainable bar level.

VI. A LOWER BOUND ON THE FRACTIONAL DISTANCE IN QUADRATIC COMPLEXITY

In [1], the following algorithm for calculating the fractional distance d_{frac} was proposed. Consider the codeword polytope $\mathcal{Q}(\mathcal{C})$ and the all-zero vertex $\mathbf{0}$. It was shown in [1] that the facets of this polytope (for plain LDPC codes) are given by (8), $\forall j \in \mathcal{J}$. Denote the set of facets of $\mathcal{Q}(\mathcal{C})$ which do not contain $\mathbf{0}$ by \mathcal{F} . For each facet $f \in \mathcal{F}$, run an LP solver to find the minimum L_1 norm $\sum_{i \in \mathcal{I}} c_i$ over f . The smallest value (over all facets) obtained in this procedure is the fractional distance [1]. The complexity of this calculation is the same as the complexity of running an LP solver $|\mathcal{F}|$ times, and in our case we have $|\mathcal{F}| = O(N)$. By using the iterative linear-complexity LP decoder, we will demonstrate a procedure which produces a lower bound on the fractional distance with complexity $O(N^2)$. In terms of computational complexity, this compares favorably with the aforementioned procedure because an LP solver in general has complexity worse than $O(N)$. Furthermore, if a higher complexity is allowed, this lower bound can be made arbitrarily close to the true fractional distance. In this section we assume plain LDPC codes. The results in the next section enable the generalization of the algorithm to GLDPC codes.

Recall that $\mathbf{c} \in \mathcal{Q}(\mathcal{C})$ if and only if $0 \leq c_i \leq 1 \ \forall i \in \mathcal{I}$ and $\forall j \in \mathcal{J}, S \subseteq \mathcal{N}_j, |S| \text{ odd}$ we have

$$\sum_{i \in \mathcal{N}_j \setminus S} c_i + \sum_{i \in S} (1 - c_i) \geq 1$$

Of these inequality constraints, the facets of $\mathcal{Q}(\mathcal{C})$ which do not contain $\mathbf{0}$ are

$$\{c_i = 1\}_{i \in \mathcal{I}} \quad (52)$$

and

$$\sum_{i \in \mathcal{N}_j \setminus S} c_i + \sum_{i \in S} (1 - c_i) = 1 \quad \forall j \in \mathcal{J}, S \subseteq \mathcal{N}_j, |S| \text{ odd}, |S| > 1 \quad (53)$$

We follow the approach in [1], i.e., for each of the facets in (52)-(53) we evaluate the minimum L_1 norm over the facet. We show how each such evaluation can be performed in linear time using Algorithm 1.

Let $i \in \mathcal{I}$ be some index and consider its corresponding facet from (52). To find the minimum weight over this facet, we can implement the method from Section V, as follows. The Tanner graph is modified by removing variable node i and all the edges incident to it. Now, to keep the graph consistent

with the original code, each constraint node $j \in \mathcal{N}_i$ (be it a standard parity check or generalized node) is modified so that it represents a local coset code $H_{j \setminus i} \mathbf{c}_{j \setminus i} = \mathbf{h}_{i,j}$ (where the subscript $j \setminus i$ denotes that we remove the i 'th column of H_j and the i 'th bit of \mathbf{c}_j) for some column vector $\mathbf{h}_{i,j} \neq 0$ rather than $H_j \mathbf{c}_j = 0$. The column $\mathbf{h}_{i,j}$ is the column from the parity-check matrix representing constraint node j , which corresponds to the index of variable node $i \in \mathcal{N}_j$ (note that if j is a standard parity check then $\mathbf{h}_{i,j} = 1$ has dimension 1). Algorithm 1 runs the same on this modified graph, except that, similarly to Section V, we need to replace the calculation of $A_{k,j}$ and $B_{k,j}$ in (28) and (29) by (44) and (45), respectively. The vector $\mathbf{h}_{i,j}$ replaces $\tilde{\mathbf{h}}^{r,c_r}$ in (44) and (45). If we take the value of the dual in the execution of Algorithm 1 then due to (18) we get for each $i \in \mathcal{I}$, a vector with weight $d_{\text{frac},i}^{(1)}$ which is a lower bound on the minimum weight over the facet $\{c_i = 1\}$. The minimum value,

$$d_{\text{frac}}^{(1)} \triangleq \min_{i \in \mathcal{I}} d_{\text{frac},i}^{(1)} \quad (54)$$

is thus a lower bound on the minimum fractional weight over all facets (52) of $\mathcal{Q}(\mathcal{C})$. This lower bound can be made as tight as desired if in Algorithm 1 we take K large enough and ϵ_0 small enough.

We now turn to the problem of calculating minimum fractional distance on the facets (53). Let r be some fixed constraint node and let $S \subseteq \mathcal{N}_r$ be an odd-sized set, $|S| > 1$. Define the hyperplane $R^{r,S}$ as follows:

$$R^{r,S} = \left\{ \mathbf{c} : \sum_{i \in \mathcal{N}_r \setminus S} c_i + \sum_{i \in S} (1 - c_i) = 1 \right\}$$

Our problem is to find the minimum fractional distance on $R^{r,S} \cap \mathcal{Q}(\mathcal{C})$, denoted $d_{\text{frac}}^{r,S}$. Consider the following problem, *Problem- $P_{\text{frac}}^{r,S,B}$* :

$$\min_{\mathbf{c}, \omega} \sum_{i \in \mathcal{I}} c_i + B \left(\sum_{i \in \mathcal{N}_r \setminus S} c_i + \sum_{i \in S} (1 - c_i) - 1 \right) \quad (55)$$

subject to (4)-(6), where $B > 0$ is some large constant. This definition is motivated by the following observations. First, the feasible region of *Problem- $P_{\text{frac}}^{r,S,B}$* (in the \mathbf{c} variables) is by definition the polytope $\mathcal{Q}(\mathcal{C})$. Thus, every feasible point must satisfy

$$\sum_{i \in \mathcal{N}_r \setminus S} c_i + \sum_{i \in S} (1 - c_i) \geq 1 \quad (56)$$

The second term in (55) is, by (56), a positive penalty term on the event of sharp inequality in (56). Therefore, in the limit where $B \rightarrow \infty$, the exact value $d_{\text{frac}}^{r,S}$ is produced as the solution to *Problem- $P_{\text{frac}}^{r,S,B}$* . If the constant B is finite, the weight $d_{\text{frac},r,S,B}^{(2)}$ of the solution to *Problem- $P_{\text{frac}}^{r,S,B}$* can be seen to be a lower bound on $d_{\text{frac}}^{r,S}$ (since the vector \mathbf{c} which attains the minimum fractional distance $d_{\text{frac}}^{r,S}$ is feasible in *Problem- $P_{\text{frac}}^{r,S,B}$* and yields the objective function value $d_{\text{frac}}^{r,S}$). Second, the objective function of *Problem- $P_{\text{frac}}^{r,S,B}$* is linear in its variables (it also contains the additive constant $B(|S| - 1)$ which is independent of the variables and thus can be ignored).

Consequently, *Problem- $P_{\text{frac}}^{r,S,B}$* can be reduced to an instance of *Problem-P*, by setting $\{\gamma_i\}_{i \in \mathcal{I}}$ as

$$\tilde{\gamma}_i = \begin{cases} 1 & i \notin \mathcal{N}_r \\ 1 - B & i \in S \\ 1 + B & i \in \mathcal{N}_r / S \end{cases} \quad (57)$$

We conclude that the solution to *Problem- $P_{\text{frac}}^{r,S,B}$* can be approximated arbitrarily closely by Algorithm 1. Now, we use Algorithm 1 to solve *Problem- $P_{\text{frac}}^{r,S,B}$* $\forall j \in \mathcal{J}, S \subseteq \mathcal{N}_j, |S| \text{ odd}, |S| > 1$. By taking the dual value output by Algorithm 1, again by (18), we obtain a set of lower bounds $\{d_{\text{frac},r,S,B}^{(2)}\}$ on the minimum fractional weight for each of the facets (53) of $\mathcal{Q}(\mathcal{C})$. A lower bound on the minimum fractional distance over the facets (53) is given by $d_{\text{frac},B}^{(2)} \triangleq \min_{r \in \mathcal{J}, S \subseteq \mathcal{N}_r, |S| \text{ odd}, |S| > 1} d_{\text{frac},r,S,B}^{(2)}$. Finally, we combine this result with (54) and obtain the lower bound

$$d_{\text{frac}} \geq d_{\text{frac},B} \triangleq \min(d_{\text{frac}}^{(1)}, d_{\text{frac},B}^{(2)})$$

Assuming the node degrees in the Tanner graph are bounded by a constant independent of N , the overall number of calls to Algorithm 1 is $O(N)$. Thus the computational complexity of evaluating a lower bound on the minimum fractional distance using the procedure described above is $O(N^2)$.

Naturally, the exact fractional distance can be approached by using very large values for the penalty constant B . It should be noted that this could theoretically have an effect on the bound on the convergence rate of Algorithm 1: In [8, Theorem 1] it was shown that the bound on the convergence rate of Algorithm 1 is related to γ_{\max} , and from (57) it can be seen that this quantity may be large as we increase B . In Section VIII, we describe several experiments conducted with $B = 10N$. In these experiments, we have not observed a significant increase in running time as compared with the minimum distance bounds from Section V.

VII. FUNDAMENTAL POLYTOPES OF GLDPC AND NONBINARY CODES

For plain LDPC codes, the fundamental polytope is represented by (8). In this section, we propose a practical procedure which obtains representations of the fundamental polytopes of two important classes of codes: GLDPC and nonbinary codes. Using these representations, one can apply a procedure similar to the one presented in Section VI to calculate a tight lower bound on the fractional distance which can be used to assess the performance of the LP decoder in these cases. An interesting effort for nonbinary codes has recently been made by Skachek [14], for ternary codes. We propose a general practical technique which relies on the double description method [9], [10] to find, similar to (8), a description of the fundamental polytope. For the case of nonbinary codes, as in [14], we consider the LP formulation from [15] which expresses a nonbinary decoding problem using a binary problem of higher dimension.

Consider a constraint node j . Suppose it represents some general, not necessarily linear, local code \mathcal{C}_j with M code-words and block length d (in what follows, we will omit the subscript j). Similar to (13) we construct a $d \times M$ matrix Ψ

for this code by writing all the codewords on the columns of that matrix, i.e.

$$\Psi = \begin{pmatrix} \mathbf{c}^0 & \mathbf{c}^1 & \dots & \mathbf{c}^{M-1} \end{pmatrix}$$

where $\mathbf{c}^0, \mathbf{c}^1, \dots, \mathbf{c}^{M-1}$ are the codewords. We also define

$$\tilde{\Psi} = \begin{pmatrix} \mathbf{1}_M \\ \Psi \end{pmatrix}$$

where $\mathbf{1}_M$ is a row vector of M ones. The code polytope, $\mathcal{Q}(\mathcal{C})$, is defined by (see Section IV for an equivalent definition)

$$\mathcal{Q}(\mathcal{C}) \triangleq \left\{ \mathbf{c} : \exists \boldsymbol{\omega} \succeq 0 \text{ such that } \tilde{\Psi} \boldsymbol{\omega} = \begin{pmatrix} 1 \\ \mathbf{c} \end{pmatrix} \right\}$$

Following [16, Theorems 4.9 and 4.10, pp. 97–98], we now show that $\mathcal{Q}(\mathcal{C})$ is indeed a polytope, and present it in a more explicit form. Consider the following two systems of linear inequalities

$$\boldsymbol{\omega} \succeq 0, \tilde{\Psi} \boldsymbol{\omega} = \begin{pmatrix} 1 \\ \mathbf{c} \end{pmatrix} \quad (58)$$

and

$$\tilde{\Psi}^T \mathbf{v} \preceq 0, (\mathbf{1} \ \mathbf{c}^T) \mathbf{v} > 0 \quad (59)$$

By Farkas' lemma (e.g. [17, page 263]) the systems (58) and (59) are strong alternatives. That is, the system (58) is feasible if and only if the system (59) is infeasible. We conclude that,

$$\mathcal{Q}(\mathcal{C}) = \{ \mathbf{c} : (\mathbf{1} \ \mathbf{c}^T) \mathbf{v} \leq 0 \ \forall \mathbf{v} \in \mathcal{T} \} \quad (60)$$

where \mathcal{T} is the following polyhedral cone

$$\mathcal{T} = \left\{ \mathbf{v} : \tilde{\Psi}^T \mathbf{v} \preceq 0 \right\} \quad (61)$$

Now, \mathcal{T} can be expressed in the following alternative form,

$$\mathcal{T} = \left\{ \mathbf{v} : \mathbf{v} = \sum_{l=1}^r \mu_l \mathbf{v}_l, \{ \mu_l \geq 0 \}_{l=1}^r \right\} \quad (62)$$

where $\mathbf{v}_l, l = 1, \dots, r$ are the extreme rays of \mathcal{T} . By [16, Proposition 4.3, p. 94] \mathbf{v}_l is an extreme ray of a polyhedral cone \mathcal{T} if and only if $\{ \eta \mathbf{v}_l : \eta \geq 0 \}$ is a one dimensional face of \mathcal{T} . For the polyhedron $\mathcal{T} \subseteq \mathbb{R}^{d+1}$, the vector $\mathbf{v} \in \mathcal{T}, \mathbf{v} \neq \mathbf{0}$ is an extreme ray if and only if it satisfies d linearly independent constraints among $\tilde{\Psi}^T \mathbf{v} \preceq 0$ with equality. By (60) and (62) we have

$$\mathcal{Q}(\mathcal{C}) = \{ \mathbf{c} : (\mathbf{1} \ \mathbf{c}^T) \mathbf{v}_j \leq 0 \ \forall j = 1, \dots, r \} \quad (63)$$

Thus, if we can obtain the extreme rays of the cone \mathcal{T} , we have the desired representation of the code polytope using (63).

One possible way of doing this is to apply the double description method [9], [10]. A pair of matrices (A, R) is said to be a double description (DD) pair if

$$A \mathbf{x} \succeq 0 \text{ iff } \mathbf{x} = R \boldsymbol{\mu}, \boldsymbol{\mu} \succeq 0 \quad (64)$$

Clearly, (61) and (62) lead to a DD pair of the cone \mathcal{T} , by identifying $A = -\tilde{\Psi}^T, \mathbf{x} = \mathbf{v}, R = (\mathbf{v}_1 \ \mathbf{v}_2 \ \dots \ \mathbf{v}_r)$ and $\boldsymbol{\mu} = (\mu_1 \ \mu_2 \ \dots \ \mu_r)^T$. The problem is, given one of the matrices R or A , to find the other. In our case, we need to find R given A . The double description method is an algorithm which solves

this problem. Unfortunately, the complexity of the algorithm in general grows exponentially with the size of the problem, so it will only work reasonably if we keep the code small. To apply the DD method, we have used the publicly available software implementation cdd+ [18].

Using cdd+, we were able to obtain a representation of a binary constraint node representing the $(7, 4)$ Hamming code \mathcal{H}_7 . The matrix $R_{\mathcal{H}_7}$ has 8 rows and 70 columns, and its transpose is given in Figure 5. For example, the first line of $R_{\mathcal{H}_7}^T$ represents the constraint

$$-2 - c_1 + c_3 + c_5 + c_7 \leq 0$$

which is a facet of $\mathcal{Q}(\mathcal{H}_7)$. Note that the constraints $0 \leq c_i \leq 1 \ \forall i \in \{1, 2, \dots, 7\}$ are also implicit in $R_{\mathcal{H}_7}$. Using this representation together with the lower bound on the fractional distance in Section VI, we found a randomly-generated GLDPC code with 70 variable nodes and 20 constraint nodes, each representing a local \mathcal{H}_7 code, with fractional distance at least 11.2418. This code has rate $1/7$. The fractional distance result guarantees that this code can correct 5 errors using the LP decoder.

Flanagan *et al.* [15] gave an LP formulation suitable for nonbinary codes over rings. For a ring $\mathcal{R} = \{0, a_1, \dots, a_{|\mathcal{R}|-1}\}$ of size $|\mathcal{R}|$, every nonbinary symbol is represented using a binary vector of size $|\mathcal{R}| - 1$. If the nonbinary symbol is zero in some codeword, the corresponding binary vector is set to zero. If the nonbinary symbol is nonzero, say a_i , then the i 'th element of the binary vector is set to 1 and the rest of the binary vector is set to zero. In this manner, a nonbinary local codeword \mathbf{c}_j is mapped to a binary local codeword. The convex hull of all the resulting binary codewords corresponding to constraint node j yields the fundamental polytope $\mathcal{Q}(\mathcal{C}_j)$ and the overall polytope is the intersection $\cap_{j \in \mathcal{J}} \mathcal{Q}(\mathcal{C}_j)$, just as in the binary case. The difference is that in the nonbinary case, the dimension of the polytope is larger, and because of the method of representation, \mathcal{C}_j , when viewed as a binary code, is not necessarily linear.

Clearly, using the DD method, it is possible to find (experimentally) the representation of any local code, provided it is not too large. As an example, using a binary vector of length 12, we have found a representation of the fundamental polytope of the nonbinary simple parity check code of length 4 over $\text{GF}(4)$. This polytope has 40 facets, given by the rows of the matrix $R_{\text{SPC}_{\text{GF}(4)}(4)}^T$, which is presented in Figure 6. For any particular LDPC code over $\text{GF}(4)$ which uses $\text{SPC}_{\text{GF}(4)}(4)$ as the local code in its constraint nodes, we can use the method in Section VI to obtain tight lower bounds on the fractional distance. The same conclusion applies in general when, instead of $\text{SPC}_{\text{GF}(4)}(4)$ we take any other code, provided that the DD method outputs (in reasonable time complexity) a representation of its corresponding fundamental polytope. We expect that this will be the case for practical constituent codes.

VIII. NUMERICAL RESULTS

In the experiments outlined below, Algorithm 1 was operated in the following mode, with respect to the values of the

$$R_{\text{SPC}_{GF(4)}(4)}^T = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ -2 & 0 & 1 & 1 & 0 & -1 & -1 & 0 & 1 & 1 & 0 & 1 & 1 \\ -2 & 0 & -1 & -1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ -2 & 1 & 0 & 1 & -1 & 0 & -1 & 1 & 0 & 1 & 1 & 0 & 1 \\ -2 & -1 & 0 & -1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ -2 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & -1 & -1 \\ -2 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & -1 & 0 & -1 \\ -1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & -1 & -1 & 0 \\ -2 & 1 & 1 & 0 & 1 & 1 & 0 & -1 & -1 & 0 & 1 & 1 & 0 \\ -2 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & -1 & 0 & 1 & 1 \\ -2 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & -1 & -1 & 0 & 1 & 1 \\ -1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 1 & 1 & 0 & -1 & -1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ -2 & -1 & -1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 & -1 & 0 & -1 & -1 & 0 & -1 & -1 & 0 & -1 \\ 0 & -1 & 0 & -1 & 1 & 0 & 1 & -1 & 0 & -1 & -1 & 0 & -1 \\ 0 & 0 & 1 & 1 & 0 & -1 & -1 & 0 & -1 & -1 & 0 & -1 & -1 \\ 0 & 0 & -1 & -1 & 0 & 1 & 1 & 0 & -1 & -1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & -1 & -1 & 0 & -1 & -1 & 0 & -1 & -1 & 0 \\ 0 & -1 & -1 & 0 & 1 & 1 & 0 & -1 & -1 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 0 & -1 & -1 & 0 & 1 & 1 & 0 & -1 & -1 \\ 0 & -1 & 0 & -1 & -1 & 0 & -1 & 1 & 0 & 1 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & -1 & 0 & -1 & -1 & 0 & -1 & 1 & 0 & 1 \\ 0 & 0 & -1 & -1 & 0 & -1 & -1 & 0 & -1 & -1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & -1 & -1 & 0 & 1 & 1 & 0 & -1 & -1 & 0 \\ 0 & -1 & -1 & 0 & -1 & -1 & 0 & -1 & -1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Fig. 6. The extreme rays of the cone \mathcal{T} of the SPC(4) code over GF(4).

parameters K and ϵ_0 . Initialize with $K = 1000$ and $\epsilon_0 = 0.01$. Iterate until $\epsilon < \epsilon_0$. Then multiply K by 1.26, divide ϵ by 1.26 and iterate with the new constraints. The process of iterating and multiplying and dividing by 1.26 is repeated ten times, so that at the end of the process $K \approx 10000$ and $\epsilon_0 \approx 0.001$.

Figure 7 shows simulation results comparing the approximate iterative LP decoder with and without merging of check nodes, as suggested in Section IV. In the simulation we picked codes at random from Gallager's (3, 6)-regular ensemble of length $N = 1002$. These codes were transmitted over a binary symmetric channel. For the merging process, check nodes are picked as follows. First, a list of short cycles (up to maximum length of 6) in the graph is generated using the procedure proposed in [19]. Based on this list, in each cycle we merge the check nodes into one new check node. This approach is motivated by Proposition 3, which guarantees an unchanged relaxation if the set of merged constraint nodes is cycle-free. As a reference, we also plot results for iterative belief propagation decoding. It is apparent from the figure that despite the improvement due to check node merging, the LP decoder exhibits worse performance than the belief propaga-

tion decoder for values of the channel crossover probability greater than 0.045, and better performance for lower values of crossover probability.

In Figure 8, we plot our results from Sections V and VI. The lower bound on the minimum distance derived in Section V is shown in circles. This plot shows, for various block lengths, the average value of \underline{l}_{\min} (see (49)) over 10 randomly-generated codes, taken from Gallager's (3, 4)-regular ensemble. We also include improved bounds obtained by merging check nodes. Check nodes were chosen for merging as in Figure 7, using all cycles of length up to 6.

Figure 8 also shows an improved lower bound on the minimum distance using the bar method outlined at the end of Section V. Clearly, in this case the lower bound is significantly improved by allowing pairs of nodes to be examined. Next, we plot the lower bound on the fractional distance from Section VI. The lower bound on the fractional distance is calculated with the penalty constant set to $B = 10N$. In this case we set ϵ_0 in Algorithm 1 to an initial value of $0.1/B$, instead of 0.01 as previously stated; this more stringent setting was used in order to increase the accuracy of our

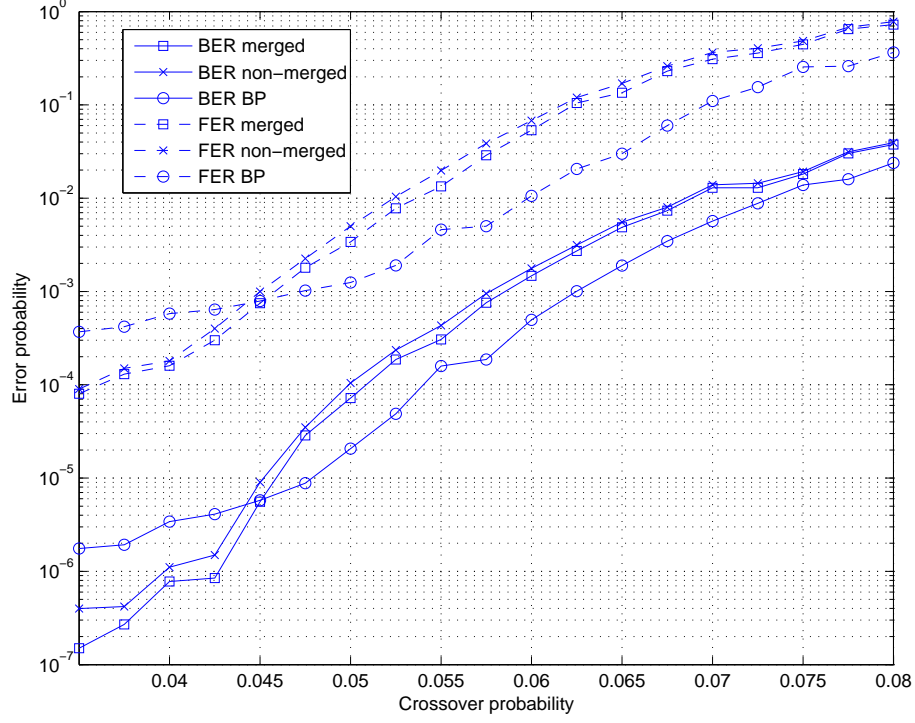


Fig. 7. Simulation results for the BSC comparing the approximate LP decoder with and without merging of check nodes with belief propagation.

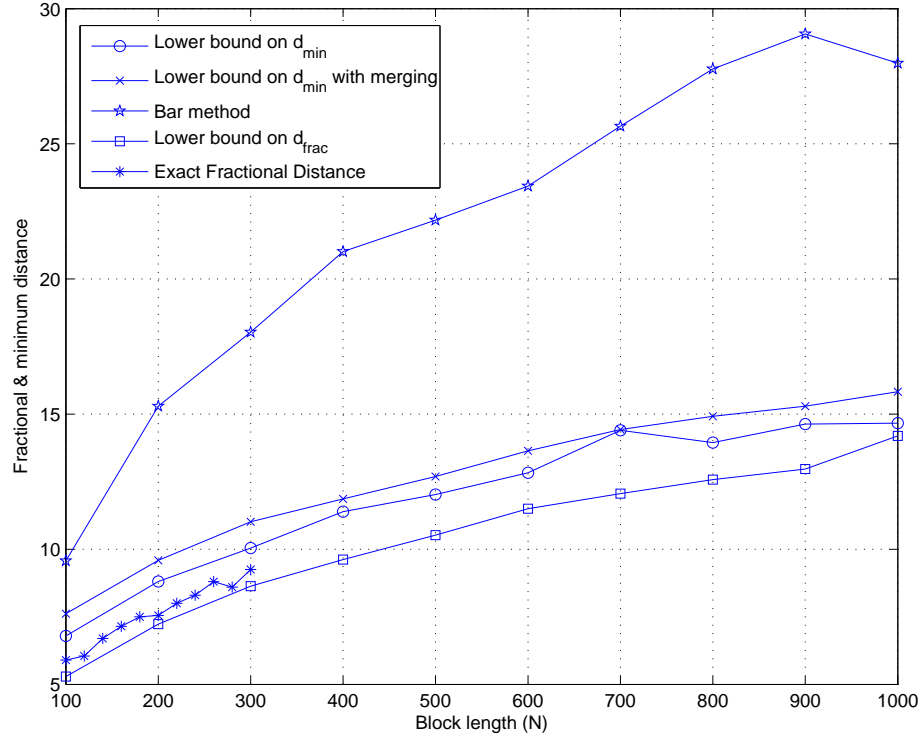


Fig. 8. Lower bounds on the fractional distance and minimum distance.

$$R_{\mathcal{H}_7}^T = \begin{pmatrix} -2 & -1 & 0 & 1 & 0 & 1 & 0 & 1 \\ -2 & 0 & -1 & 1 & 0 & 0 & 1 & 1 \\ -2 & 0 & -1 & 1 & 1 & 1 & 0 & 0 \\ -2 & -1 & 0 & 1 & 1 & 0 & 1 & 0 \\ -2 & -1 & 1 & 0 & 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ -2 & 0 & 0 & 0 & -1 & 1 & 1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -2 & 0 & 0 & 0 & 1 & 1 & 1 & -1 \\ -2 & 1 & -1 & 0 & 0 & 1 & 1 & 0 \\ -2 & 0 & 1 & -1 & 0 & 0 & 1 & 1 \\ -2 & 0 & 1 & -1 & 1 & 1 & 0 & 0 \\ -2 & 1 & 0 & -1 & 0 & 1 & 0 & 1 \\ -2 & 1 & 0 & -1 & 1 & 0 & 1 & 0 \\ -2 & 1 & -1 & 0 & 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ -2 & 0 & 0 & 0 & 1 & -1 & 1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -2 & 0 & 0 & 0 & 1 & 1 & -1 & 1 \\ -2 & -1 & 1 & 0 & 1 & 0 & 0 & 1 \\ -2 & 0 & 1 & 1 & 0 & 0 & -1 & 1 \\ -2 & 1 & 0 & 1 & 0 & -1 & 0 & 1 \\ -2 & 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ -2 & 0 & 1 & 1 & 1 & -1 & 0 & 0 \\ -2 & 1 & 1 & 0 & 0 & -1 & 1 & 0 \\ -2 & 1 & 1 & 0 & 1 & 0 & 0 & -1 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 1 & 1 & 0 & -1 & 0 & 0 & 1 \\ -2 & 1 & 1 & 0 & 0 & 1 & -1 & 0 \\ -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ -2 & 0 & 1 & 1 & -1 & 1 & 0 & 0 \\ -2 & 1 & 0 & 1 & -1 & 0 & 1 & 0 \\ -2 & 1 & 0 & 1 & 0 & 1 & 0 & -1 \\ -2 & 0 & 1 & 1 & 0 & 0 & 1 & -1 \\ -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & -1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 1 & -1 & -1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & -1 & -1 \\ 0 & -1 & 0 & 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 & -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & -1 & -1 \\ 0 & 1 & 0 & -1 & 0 & -1 & 0 & -1 \\ 0 & 1 & -1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & -1 & 1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & -1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 0 & 0 & -1 & 1 \\ 0 & -1 & 0 & -1 & 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & -1 & 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & -1 & -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 & 0 & 1 & 0 & -1 \\ 0 & -1 & 0 & -1 & -1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 1 & 0 & 0 & -1 \\ 0 & -1 & -1 & 0 & 0 & -1 & 1 & 0 \\ 0 & -1 & -1 & 0 & 0 & 1 & -1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Fig. 5. The extreme rays of the cone \mathcal{T} of the $(7, 4)$ Hamming code.

result in light of the large value of γ_{\max}^2 . Finally, exact fractional distance results, appearing in asterisks, are included in Figure 8. These results were taken from [1] and depict exact fractional distance, averaged over a sample of 100 codes. With the exception of these exact results from [1], all results depict the average over the same 10 randomly-generated codes, taken from Gallager's $(3, 4)$ -regular ensemble. Comparing the exact results with our lower bound, we see that although the randomly-selected codes are not the same, the statistical averages indicate that the lower bound is close to the mark for $B = 10N$.

IX. CONCLUSION

In this paper we made obtained the following contributions to the framework of LP decoding. First, a method for improving LP decoding based on merging check nodes was proposed. Second, an algorithm for determining a lower bound on the minimum distance was presented. This algorithm can be improved by the check node merging technique or by the greedy procedure introduced in Section V. This algorithm has computation complexity $O(N^2)$, where N is the block length. Third, an algorithm for determining a tight lower bound on the minimum distance was presented. This algorithm also has complexity $O(N^2)$. Fourth, we showed how the fundamental polytope can be obtained for GLDPC and nonbinary codes.

REFERENCES

- [1] J. Feldman, M. J. Wainwright, and D. R. Karger, "Using linear programming to decode binary linear codes," *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 954–972, Mar 2005.
- [2] S. C. Draper, J. S. Yedidia, and Y. Wang, "ML decoding via mixed-integer adaptive linear programming," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2007)*, Nice, France, June 2007.
- [3] M. H. Taghavi and P. H. Siegel, "Adaptive methods for linear programming decoding," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5396–5410, December 2008.
- [4] A. G. Dimakis, A. A. Gohari, and M. J. Wainwright, "Guessing facets: polytope structure and improved LP decoding," *IEEE Transactions on Information Theory*, vol. 55, no. 8, pp. 3479–3487, August 2009.
- [5] P. O. Vontobel and R. Koetter, "Towards low-complexity linear-programming decoding," in *Proc. 4th Int. Symposium on Turbo Codes and Related Topics*, Munich, Germany, April 2006, arxiv:cs/0602088v1.
- [6] P. O. Vontobel and R. Koetter, "On low-complexity linear-programming decoding of LDPC codes," *European Transactions on Telecommunications*, vol. 18, no. 5, pp. 509–517, August 2007.
- [7] K. Yang, X. Wang, and J. Feldman, "A new linear programming approach to decoding linear block codes," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 1061–1072, Mar 2008.
- [8] D. Burshtein, "Iterative approximate linear programming decoding of LDPC codes with linear complexity," *IEEE Transactions on Information Theory*, vol. 55, no. 11, pp. 4835–4859, November 2009.
- [9] K. Fukuda and A. Prodon, "Double Description Method Revisited," *Report, ETHZ Zürich, Available: <http://ftp.ifor.math.ethz.ch/pub/fukuda/paper/ddrev960315.ps.gz>*, 1995.
- [10] T. S. Motzkin, H. Raiffa, G. L. Thompson, and R. M. Thrall, "The double description method," *Contributions to the theory of games*, vol. 2, pp. 51–73, 1953.
- [11] J.K. Wolf, "Efficient maximum likelihood decoding of linear block codes using a trellis," *IEEE Transactions on Information Theory*, vol. 24, no. 1, pp. 76–80, January 1978.
- [12] C. Hartmann and L. Rudolph, "An optimum symbol-by-symbol decoding rule for linear codes," *IEEE Transactions on Information Theory*, vol. 22, no. 5, pp. 514–517, September 1976.

²This is the setting which could potentially have the effect on the convergence rate of Algorithm 1 which was discussed in the end of Section VI.

- [13] D. Bertsekas, *Convex Analysis and Optimization*, Athena Scientific, Belmont, Mass., 2003.
- [14] V. Skachek, "Characterization of graph-cover pseudocodewords of codes over F_3 ," in *Proceedings of the IEEE Information Theory Workshop (ITW 2010)*, Dublin, Ireland, September 2010.
- [15] M. F. Flanagan, V. Skachek, E. Byrne, and M. Greferath, "Linear-programming decoding of nonbinary linear codes," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4131–4154, September 2009.
- [16] G. L. Nemhauser and L. A. Wolsey, *Integer and Combinatorial Optimization*, Wiley, New York, 1988.
- [17] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, Cambridge, UK, 2004.
- [18] K. Fukuda, "CDD and CDD+ homepage," http://www.ifor.math.ethz.ch/~fukuda/cdd_home/cdd.html, 2008.
- [19] James C. Tiernan, "An efficient search algorithm to find the elementary circuits of a graph," *Commun. ACM*, vol. 13, no. 12, pp. 722–726, 1970.